Vermont Age-Appropriate Design Code

Public Written Comments — Consolidated Record

All 32 submissions listed on the Vermont Attorney General's Office Age-Appropriate Design Code Rulemaking Feedback page, including informal submissions. The original PDF pages follow this index without alteration. This compilation is identical for the § 2449f and § 2449g packets.

Index of submissions

01. Comments on Rule 26P027.pdf **— p. 2** (1 page)

02. ESA Vermont AADC Comments - 3.16.2026 (final-signed) (1).pdf **— p. 3** (6 pages)

03. KGI - Vermont AADC Rulemaking Informal Input - 01-13-2026 (1).pdf **— p. 9** (13 pages)

04. Age-Appropriate Design Comments 9-9-26.pdf **— p. 22** (1 page)

05. Technical Input - Vermont Age-Appropriate Design Code - Age Assurance, Interoperability & Verifiable Youth-Safety Controls 9-9-26.pdf **— p. 23** (2 pages)

06. Technical Comments - Vermont Age-Appropriate Design Code Rulemaking - CIVITERA GOVTECH INC..pdf **— p. 25** (11 pages)

07. CCIA Comments_AGO Age Appropriate Design Code Proposed Regulations.pdf **— p. 36** (16 pages)

08. Comment from Front Porch Forum re Act 63 rulemaking 9-24-26.pdf **— p. 52** (3 pages)

09. KGI Comments on Vermont AADC Rulemaking, Sections 2449g 9-25-26.pdf **— p. 55** (26 pages)

10. Comment on proposed rule, 9 V.S.A. § 2449f (Prohibited Data and Design Practices) 9-25-26.pdf **— p. 81** (3 pages)

11. Public Comment on Proposed Rule 26P027 9-27-26.pdf **— p. 84** (3 pages)

12. Solid Rules 9-28-26.pdf **— p. 87** (1 page)

13. Written Comment to rule change on technology use and minors 9-29-26.pdf **— p. 88** (2 pages)

14. Public Comment on Sections 2249f and 2449g of Act 63 9-28-26.pdf **— p. 90** (1 page)

15. Comment on the proposed Age Assurance Privacy rule (9 V.S.A. § 2449g) 9-30-26.pdf **— p. 91** (2 pages)

16. TechNet AADC Proposed Rule Comments 10-1-26.pdf **— p. 93** (5 pages)

17. SIIA Comments on VT AADC Rulemaking 10-1-26.pdf **— p. 98** (6 pages)

18. AADC Draft Rules - Motion Picture Association Comments 10-1-26.pdf **— p. 104** (10 pages)

19. Ad Trade Opposition to Vermont AADC Rulemaking 10-2-26.pdf **— p. 114** (5 pages)

20. Vermont AADC Rulemaking Submission - Future of Privacy Forum 10-2-26.pdf **— p. 119** (13 pages)

21. NECTA Comments on Proposed rules for Sections 2249f and 2449g of Act 63 10-2-26.pdf **— p. 132** (10 pages)

22. comments on proposed rules for Act 63, An Act Relating to an Age-Appropriate Design Code 10-2-26.pdf **— p. 142** (6 pages)

23. Internet Works Vermont AADC Comments 10-2-26.pdf **— p. 148** (4 pages)

24. Age-Appropriate Design Code Comment Letter 10-2-26.pdf **— p. 152** (4 pages)

25. State Privacy and Security Coalition Comments on Proposed Rules 26P027 and 26P028 10-2-26.pdf **— p. 156** (23 pages)

26. Vermont AADC Rulemaking - Entertainment Software Association (ESA) Comments 10-2-26.pdf **— p. 179** (10 pages)

27. Vermont AADC Rulemaking Submission - Electronic Privacy Information Center (EPIC) 10-2-26.pdf **— p. 189** (31 pages)

28. Common Sense Media Comments in Response to Vermont Age-Appropriate Design Code Rulemaking 10-2-26.pdf **— p. 220** (8 pages)

29. Comments from the NAI Re Proposed Rules for Sections 2249f of the Vermont Age-Appropriate Design Code 10-2-26.pdf **— p. 228** (7 pages)

30. ACT Comments on the Vermont AADC Proposed Rules 10-2-26.pdf **— p. 235** (3 pages)

31. Age-Appropriate Design Code Rule-making 10-2-26.pdf **— p. 238** (10 pages)

32. MAMA Comments on Vermont Age-Appropriate Design Code Rulemaking 10-2-26.pdf **— p. 248** (3 pages)

From: vt-noreply@egov.com
To: Jameson, Sarah
Subject: Comments on Rule 26P027
Date: Sunday, August 16, 2026 1:40:33 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Comments on Rule 26P027
Reply To:john.h.starkie@gmail.com
The same design choices that are harmful to minors are also harmful to certain disabled adults, people with gambling addictions, and anyone with ADHD. Why give them the power to target these groups when we could protect everyone from their predatory behavior.

March 16, 2026

Attorney General's Office
ATTN: Vermont Age-Appropriate Design Code Act
109 State Street
Montpelier, VT 05609

Comments of the Entertainment Software Association
Regarding the Vermont Age-Appropriate Design Code Act

The Entertainment Software Association[1] ("ESA") appreciates the opportunity to submit comments to the Attorney General's Office regarding the Vermont Age-Appropriate Design Code Act ("AADC"). ESA is committed to helping young Vermonters have safe and positive online experiences. We share the Attorney General's interest in promoting policies that will allow Vermonters of all ages to enjoy access to online experiences that are safe, fun, and rewarding.

ESA respectfully provides the following comments to help the Attorney General develop policies that will advance these goals. In our experience, to support age-appropriate design, it is important for regulations to be flexible and proportionate to the relevant risks (reflecting, for example, the differences among young people, evolving nature of technology, and other factors), and empowering for parents, who are positioned best to decide what is right for their families. We would be glad to discuss these views and our experience with the Attorney General.

I. Vermonters of all ages and from all backgrounds enjoy playing video games.

A wide range of research shows that people from all walks of life play video games for fun, and that video games can benefit a person's mental, emotional, and social well-being in remarkable ways.

Vermonters play video games to have fun and de-stress, as do most video game players across the world. For example, an Oxford University study involving more than 80,000 players reported that their findings "corroborate what qualitative research and reports from video game players around the world have long suggested: people feel good playing games."[2] Positive

[1] ESA is the U.S. trade association for companies that publish interactive entertainment software for video game consoles, handheld devices, personal computers, and the internet. Our members not only create some of the world's most engaging interactive experiences for consumers, but also develop novel technologies that are at the cutting edge, such as virtual, augmented, and mixed reality hardware and software as well as the latest consoles and handheld video game devices.

[2] ESA, Power of Play: 2025 Global Video Games Report (2025), https://www.theesa.com/resources/the-global-power-of-play-report (quoting Vuorre, M., Ballou, N., Hakman, T., Magnusson, K., & Przybylski, A. K. (2023). Affective uplift during video game play: A naturalistic case study. [PREPRINT]); *see also id.* ("[G]aming may be among the most efficient and effective means by which children and youth generate positive feelings.") (quoting Granic, I., Lobel, A., & Engels, R. C. (2014). The benefits of playing video games. *American Psychologist*, 69(1), 66–78)).

impacts of gameplay surpassed mood improvements from watching television, reading, and shopping.[3]

Research also shows the cognitive, motivational, emotional, and social benefits tied to video games. In fact, research published in *American Psychologist*, the American Psychological Association's academic journal, notes that researchers have been "particularly inspired by the potential that these games hold for interventions that promote well-being, including the prevention and treatment of mental health problems in youth."[4] Other research has noted that "video gameplay gives gamers the chance to develop techniques for dealing with conflict, working out various resolutions, interacting with their friends, and experiencing different emotions."[5] Moreover, "[c]ognitive skills such as perception, attentional control, and decision-making improve when subjects were trained with video games," and "students who played video games exhibit better results when given tasks related to cognitive abilities compared to students who do not play video games."[6]

Video games bring joy and a sense of belonging to Vermonters from all backgrounds. Two thirds of Americans—people of all ages, ethnicities, races, gender identities and backgrounds—play video games.[7] Nearly half of all players identify as female, and the majority of Gen Alpha, Gen Z, and Millennials play video games, along with roughly half of Gen X and Boomers.[8] Seventy percent of Americans agree that video games can bring different types of people together, and 74% say that video games provide accessible experiences for people with different abilities.[9] By expanding the possibilities for storytelling, video games often enable players to visualize themselves in a narrative. For example, this can take the form of players creating an avatar to reflect chosen aspects of identity or even look like no character at all—simply taking control of a race car or a first-person adventure as themselves. In these ways, video games foster creativity, individuality, and self-expression.

---

[3] *Id.*

[4] *Id.* (quoting Granic, I., Lobel, A., & Engels, R. C. (2014). The benefits of playing video games. *American Psychologist,* 69(1), 66–78).

[5] *Id.* (quoting Markey, P. M., Ferguson, C.J., & Hopkins, L.I. (2020). Video game play: Myths and benefits. *American Journal of Play*, 13(1), 87–106).

[6] *Id.* (quoting Reynaldo, C., Christian, R., Hosea, H., & Gunawan, A. A. S. (2021). Using video games to improve capabilities in decision making and cognitive skill: A literature review. *Procedia Computer Science*, 179, 211–221).

[7] *Inclusion &* Belonging, Ent. Software Ass'n, https://www.theesa.com/issues/inclusion-belonging (last visited Mar. 11, 2026).

[8] *Id.*

[9] *Id.*

II. The video game industry has adopted leading protections for privacy and online safety.

The video game industry has taken robust steps to protect privacy and promote online safety. These steps include highly regarded certification programs and providing players and families with transparency, choice, and control over personal information and digital experiences.

For example, the Entertainment Software Rating Board ("ESRB"), the video game industry's self-regulatory body since 1994, operates Privacy Certified, a privacy compliance and certification program approved by the U.S. Federal Trade Commission ("FTC").[10] The program's General Seal Requirements are based on federal and state law, regulatory enforcement, and global best practices, incorporating principles such as transparency and notice, consent and choice, data minimization, and accountability. These standards require companies to give consumers clear and accurate information regarding (i) how their personal information is collected, used, and shared, and (ii) how to make privacy choices and exercise relevant consumer data rights.[11] ESRB's Kids Seal Requirements similarly integrate provisions of the U.S. Children's Online Privacy Protection Act ("COPPA") and reflect insights from FTC and state enforcement actions and FTC guidance.[12]

ESA members are also leaders in online safety. For example, the FTC has lauded the industry's efforts to responsibly market its products and noted that the industry "outpaces" other entertainment sectors in having the "strongest self-regulatory code" and "high compliance" with that code.[13] ESA and its members also partner with organizations to facilitate information sharing and coordination, such as groups like the National Center for Missing & Exploited Children, Family Online Safety Institute, Games for Change, Raising Good Gamers, Safer Internet Day, and Fair Play Alliance.[14]

Vermont families benefit from a variety of online safety controls that ESA member companies have developed, including filtering by age rating, limiting the visibility of personal information, managing the time or money kids can spend playing video games, and restricting, blocking, or reporting player-to-player communications (including customized options for muting certain words). Virtually all devices—including consoles, smartphones, tablets and PCs—

---

[10] *Privacy*, ESRB, https://www.esrb.org/privacy (last visited Mar. 11, 2026).

[11] *Privacy Certified Seals*, ESRB, https://www.esrb.org/privacy-certified-seals (last visited Mar. 11, 2026).

[12] *Id.*

[13] FTC, Marketing Violent Entertainment to Children: A Sixth Follow-up Review of Industry Practices in the Motion Picture, Music Recording & Electronic Game Industries, at iii, 24, 30 (2009), https://www.ftc.gov/sites/default/files/documents/reports/marketing-violent-entertainment-children-sixth-follow-review-industry-practices-motion-picture-music/p994511violententertainment.pdf.

[14] *Protecting players by working together*, Ent. Software Ass'n, https://www.theesa.com/trust-safety/working-in-partnership (last visited Mar. 11, 2026).

provide controls to manage video gameplay.[15] ESRB helps parents to make informed decisions by providing age ratings and descriptions of content and interactive elements in games.[16] ESRB also provides a centralized place with step-by-step control guides for consoles, Windows computers, and other platforms.[17]

These efforts seek to promote "positive play" so that players enjoy a game experience based on sportsmanship, camaraderie, and mutual respect. Games use a wide variety of methods to support positive communities consistent with a company's objectives and approach to expression. For instance, member companies have codes of conduct that set expectations for players and may articulate specific values, such as respect, integrity, fairness, or fun.[18] Mechanisms to encourage positive values include incentive systems for positive behaviors, penalties for offensive chats, or warning systems to address disruptive players.

III. Regulations that are flexible, proportionate to risks, and empowering for families will help young Vermonters to enjoy safe and positive online experiences.

In our experience, it is important for online safety regulations to be flexible, proportionate to risks, and empowering for parents. This type of approach is valuable because every Vermont family is different, making one-size-fits-all requirements inappropriate, and overly prescriptive regulations can undermine privacy and safety protections.

Legal requirements should reflect the principle that parents are best equipped to assess the needs of their children. No two Vermont children or families are the same. Regulations should therefore allow parents to guide a video game player's online experience, rather than dictating to parents what is best for their families. This will lead to better safety outcomes and more positive online experiences because families can determine what makes the most sense for their own circumstances. Families can assist in building children's digital literacy and allow them to "age-up" appropriately as they move from being children to adults.

Overly prescriptive regulations can also be counterproductive for several reasons, undermining privacy and safety protections. To start, safety measures are most effective when there is some buy-in from users. If users experience too much friction from new requirements, they may begin to use services or technology in unintended ways (e.g., users might use VPNs to avoid age assurance or parents could share accounts to avoid hassle).

---

[15] *Trust and Safety: Parental Controls*, Ent. Software Ass'n, https://www.theesa.com/trust-safety/parent-controls (last visited Mar. 11, 2026).

[16] *Ratings Guide*, ESRB, https://www.esrb.org/ratings-guide.

[17] *Tools for Parents*, ESRB, https://www.esrb.org/tools-for-parents (last visited Mar. 11, 2026).

[18] *Trust and Safety: Setting guidelines for acceptable online behavior*, Ent. Software Ass'n, https://www.theesa.com/trust-safety/codes-of-conduct (last visited Mar. 11, 2026).

Overly prescriptive requirements can also undermine accountability. For example, when requirements are highly prescriptive, businesses may focus on ticking boxes to meet minimum requirements rather than genuinely managing risks. Prescriptive rules can also make it more difficult for consumers to understand what role a company plays in ensuring safety, versus what is mandated by law, eroding informed consumer choice and reducing further the incentive for companies to go beyond the minimum requirements.

Moreover, overly prescriptive regulations tend to be incompatible with technologies that are constantly changing and improving. Rigid regulations can quickly become outdated, thus failing to promote safety over the long term. They can also hinder innovation aimed at improving safety outcomes. For example, ESA members enhance their safety protocols by integrating research, new design approaches, and insights from players. Some companies use artificial intelligence to detect cheating or help with blocking chats that violate codes of conduct (e.g., hate speech, discriminatory language, or harassment).[19] Companies are also using image-hashing technology and machine learning to look out for harms like child exploitation.[20] Flexible requirements allow and encourage companies to continue improving safety measures in this manner. By contrast, prescriptive requirements can stifle innovation, as businesses are less likely to seek better solutions if they are only required to follow set procedures or may be stuck using measures that the law requires but that could be substituted for better approaches.

Flexible and proportionate requirements are additionally important to support creativity and free expression, helping Vermonters enjoy access to rewarding, lawful online experiences. For example, video games allow users to explore other worlds and be awed by epic stories. Regulations should seek to foster this type of creative expression, providing Vermonters with access to exciting opportunities for learning, play, and wonder.

Prescriptive requirements may run afoul of the First Amendment, which protects the speech rights of video game players and developers. The Supreme Court has explained that video games are expressive works, similar to newspapers, books, movies, or music in this respect.[21] As the Supreme Court noted, "video games communicate ideas—and even social messages—through many familiar literary devices (such as characters, dialogue, plot, and music) and through features distinctive to the medium (such as the player's interaction with the virtual world)."[22] Courts have found that many online safety requirements violate the First Amendment and other constitutional provisions. AADCs have already been legally challenged in several states, and several provisions of California's AADC have been found likely unconstitutional, while courts continue to sort through other parts of the California AADC and

---

[19] *Artificial Intelligence*, Ent. Software Ass'n, https://www.theesa.com/issues/ai (last visited Mar. 11, 2026).

[20] *Id.*

[21] *Brown v. Ent. Merchants Ass'n*, 564 U.S. 786, 790 (2011).

[22] *Id.*

other AADCs.[23] Courts have also enjoined a wide variety of other online safety legislation due to First Amendment and vagueness concerns.[24]

Conclusion

Vermonters of all ages enjoy video games and benefit from the video game industry's leading privacy and online safety measures. Regulations that are flexible, proportionate to risks, and empowering for families can help young Vermonters have safe and positive online experiences. ESA welcomes the opportunity to discuss these views and our experience further with the Attorney General.

Respectfully submitted,

Michael G. Lewis

Associate General Counsel, Law and Policy

[23] *NetChoice, LLC v. Bonta*, No. 25-2366, 2026 WL 694471, at *14 (9th Cir. Mar. 12, 2026) (noting, among other things, unconstitutionally vague data restrictions); *NetChoice v. Brown*, No. CV RDB-25-0322, 2025 WL 3267786 (D. Md. Nov. 24, 2025) (denying Maryland's motion to dismiss); Compl., *NetChoice v. Wilson*, No. 3:26-cv-00543-SAL (D.S.C. Feb. 9, 2026) (challenging South Carolina AADC).

[24] *See, e.g.*, *NetChoice v. Jones*, No. 1:25-CV-2067 (PTG/LRV), 2026 WL 561099 (E.D. Va. Feb. 27, 2026); *NetChoice, LLC v. Weiser*, No. 25-cv-2538-WJM-KAS, 2025 WL 3101019 (D. Colo. Nov. 6, 2025).

Knight Georgetown Institute

JANUARY 2026

Knight-Georgetown Institute (KGI) Informal Input on the Vermont Age-Appropriate Design Code Rulemaking

I. Introduction

The Knight-Georgetown Institute (KGI) is dedicated to connecting independent research with technology policy and design. Based at Georgetown University in Washington, D.C., KGI serves as a central hub for the growing network of scholarship that seeks to shape how technology is used to produce, disseminate, and access information. KGI is designed to provide practical resources that policymakers, journalists, and private and public sector leaders can use to tackle information and technology issues in real time.

We welcome the opportunity to inform the Vermont Age-Appropriate Design Code (AADC) Rulemaking and appreciate the Attorney General's engagement with independent research and implementation considerations in this process. This comment draws on interdisciplinary research examining how specific features and other elements of platform product design can affect the well-being of users, particularly children and adolescents, as well as technical insights relevant to the deployment of age assurance systems. Our aim is to highlight potential risks associated with certain design practices and to identify best practices for the implementation of age assurance requirements.

Section I of this comment addresses platform product design and responds to questions 10 and 12; Section II focuses on age assurance and is responsive to questions 21, 22, 29, 31, and 35.

II. Design Practices and Compulsive Use

Given the reality of cognitive development in minors, numerous scholars have conducted research on the experiences of adolescents in digital environments. While digital platform use can deliver benefits to young people, current science also suggests that certain features of social media can be harmful to the health of some adolescents.[1]

When considering design practices in questions 10 and 12, the Vermont Attorney General's Office (AGO) may consider relevant research related to specific design features and compulsive use. This section summarizes key research relevant to specific design practices.

A. Infinite Scroll

Infinite scroll is a common platform feature where content automatically and continuously loads at the bottom of a screen. Researchers contend that this platform design element "monetizes the same human tendency that was illustrated by the famous 'bottomless bowl of soup' experiment," where research subjects who had their soup bowls automatically and unknowingly refilled consumed significantly more than subjects who had to affirmatively ask for more.[2] Studies of infinite scroll have documented a tendency to cause a loss of control among users and, in combination with other features, can drive extended, unintentional periods of platform engagement.[3] This occurs because, during bursts of user engagement, users can enter "flow states"—sustained periods of heightened concentration in which users experience enjoyment and time distortion—that are associated with subsequent regret and, potentially, development of problematic social media use.[4]

B. Autoplay

Autoplay causes videos to play continuously in a sequence without user engagement. A 2021 survey of YouTube users found that autoplay leads to a loss of control and sense of user agency and increased the amount of time spent on the site.[5]

Autoplay has been empirically shown to extend users' viewing time on their devices.[6] For example, a 2024 study suggests that disabling Netflix's autoplay feature led to 21 fewer minutes watched each day and 17-minute shorter sessions on average.[7] A study focused specifically on preschoolers found

[1] See, e.g., American Psychological Association, "'Potential Risks of Content, Features, and Functions."
[2] Langvardt, "Regulating Habit-Forming Technology"; Rixen et al., "The Loop and Reasons to Break It"; Wansink et al., "Bottomless Bowls."
[3] Cho et al., "Reflect, Not Regret"; Natarajan, "Do They Stop?"; Park and Jung, "Unveiling the dynamics of binge-scrolling."
[4] Rixen et al., "The Loop and Reasons to Break It"; Roberts and David, "Instagram and TikTok Flow States and Their Association with Psychological Well-Being"; Qin et al., "Flow Experience Is a Key Factor in the Likelihood of Adolescents' Problematic TikTok Use."
[5] Cho et al., "Reflect, Not Regret"; Lukoff et al., "How the Design of YouTube Influences User Sense of Agency."
[6] Schaffner et al., "An Experimental Study of Netflix Use and the Effects of Autoplay on Watching Behaviors."
[7] Ibid.

that autoplay extended children's viewing time.[8] Autoplay is also strongly associated with negative emotions such as higher levels of regret, procrastination, and dissatisfaction after an excessive viewing session.[9]

C. Engagement Gamification

Engagement is "gamified" through visible indicators of engagement (e.g., likes, reactions, like counts, or reaction counts) as well as streaks and goals that encourage continuing use. A 2015 review of gamification literature highlighted how such approaches are rooted in psychology to motivate user engagement.[10]

Longitudinal research indicates that the minors most vulnerable to developing problematic social media use may be those with higher levels of social comparison and lower levels of social support, who compensate by spending more time online.[11] By deepening social comparison with peers, engagement gamification has the potential to exacerbate these risks. For instance, platform features such as streaks, likes, or visible like counts may cause "fear of missing out" on being seen as popular or interesting when the number of reactions is unexpected.[12] Token rewards are another form of engagement gamification which have been found to increase the willingness to share content online.[13]

Engagement gamification may also involve sharing of personal details and profile content when setting up and using a social media account. This identity feature could facilitate craving and loneliness when individuals interact on social media to maintain their self-concept, which can also lead to comparisons of profiles, causing low self-esteem.[14] In addition to identity on profiles, user avatars can also be an essential element of engagement gamification. Study results have noted positive feelings such as affection, connection with their avatars, and increased identification with avatars.[15]

Hiding engagement metrics such as likes and comments in an experimental study led to decreased time on social media.[16]

[8] Hiniker et al., "Coco's Videos."
[9] Chaudhary et al., "'Are You Still Watching?'"
[10] Seaborn and Fels, "Gamification in theory and action."
[11] Salerno et al., "Social support and social comparison tendencies predict trajectories of adolescents' problematic social media use."
[12] Alutaybi et al., "Designing social networks to combat fear of missing out"; Bernstein, "Unwired," 37.
[13] Alizadeh et al., "Tokenization of social media engagements increases the sharing of false (and other) news but penalization moderates it."
[14] Altuwairiqi et al., "When People Are Problematically Attached to Social Media."
[15] Suh et al., "What If Your Avatar Looks Like You?"
[16] Roffarello and De Russis, "Towards Understanding the Dark Patterns That Steal Our Attention."

D. Notifications

Online platforms send notifications of both platform and third-party content designed to pull users to the app or site. The timing and use of such notifications have been described as a tool of distraction and intermittent reward.[17]

Studies of social media users have found that notifications contribute to increased use.[18] Push notifications can also contribute to problematic attachment and a significantly higher level of usage of social media platforms, by creating a sense of urgency and anxiety.[19] Platforms often make changing default settings for notifications complex.[20]

In addition, researchers have raised concerns that push notifications can exacerbate nighttime use of smartphones by minors, which can displace and lower the quality of sleep.[21] One recent empirical study found that such usage of smartphones is associated with attentional problems during the day and worse performance at school among teens.[22]

E. Barriers to Account Deletion

Researchers have shown that many social media platforms introduce barriers (so-called dark or deceptive patterns) to account deletion, including complex user interfaces and delayed deletion of account data.[23] The study examined account deletion flows and interfaces of the top 20 most popular social media platforms and then surveyed users about their experiences, finding that while successfully completed deletion was the most common outcome (64.5% of attempts), many users changed their mind (47.1%), could not find the account deletion option (17.4%), and/or gave up because it was too tedious or complicated (16.5%).[24]

Ongoing US litigation has further shown that Facebook and TikTok require a 30-day delay before a user can affirmatively delete their account.[25] Legal complaints suggest that users must navigate seven different pages and pop-ups to delete a Facebook account.[26]

---

[17] Ibid, 36; Fitz et al., "Batching smartphone notifications can improve well-being"; Salo et al., "Technostress and social networking services."
[18] Brown and Kuss, "Fear of Missing Out, Mental Wellbeing, and Social Connectedness"; Griffiths, "Adolescent social networking."
[19] Altuwairiqi et al., "When People Are Problematically Attached to Social Media"; Salo et al., "Technostress and social networking services."
[20] Office of Minnesota Attorney General, "Minnesota Attorney General's Report on Emerging Technology and Its Effects on Youth Well-Being.'
[21] Stevic et al., "Distracted children?"
[22] Ibid.
[23] Schaffner et al., "Understanding Account Deletion and Relevant Dark Patterns on Social Media."
[24] Ibid.
[25] Lawrence, "Public Health Law's Digital Frontier"; United States District Court for the Northern District of California, "Plaintiff's Amended Master Complaint."
[26] United States District Court for the Northern District of California, "Plaintiff's Amended Master Complaint."

F. Variable or Intermittent Rewards

Variable or intermittent rewards relate to the timing and sequencing of notifications, social feedback, and other design features, including "positive stimuli provided at random intervals."[27] Researchers have noted that digital platforms deploy these techniques to retain our attention.[28] Research has also documented the presence of variable and intermittent rewards within various platform design elements, including recommended content feeds and push notifications.[29] These strategies can contribute to dependence and habit formation over time—analogous to tactics deployed in the gambling industry.[30] A 2022 study found that platform habit formation tools like intermittent rewards drive social media use.[31]

III. Age Assurance

A. Age Assurance Methods

Age assurance methods are conventionally broken down into three broad categories, as described in ISO/IEC 27566-1:[32]

- *Age estimation* methods, which use a user's physical characteristics (e.g., their facial features) to produce an estimate of their age.
- *Age inference*[33] methods, which attempt to match up user identifying information (e.g., a name or email address) with various governmental and private records in order to determine whether the user is in the appropriate age range.
- *Age verification* methods, which use some form of user identification (e.g., a government ID) to determine a user's age.

Each of these categories encompasses multiple potential methods. For example, the table below shows the methods provided by the UK-based verification provider Yoti:[34]

[27] Burhan and Moradzadeh, "Neurotransmitter Dopamine (DA) and its Role in the Development of Social Media Addiction."
[28] Bernstein, "Unwired," 36.
[29] Ibid; Cho et al., "Reflect, Not Regret"; Qin et al., "Flow Experience Is a Key Factor in the Likelihood of Adolescents' Problematic TikTok Use"; Rixen et al., "The Loop and Reasons to Break It"; Salo et al., "Technostress and social networking services."
[30] Ibid.; Bernstein, "Unwired," 37; Zeiler, "Fixed-interval behavior."
[31] Allcott et al., "Digital Addiction"; Office of the Surgeon General, "Social Media and Youth Mental Health."
[32] International Organization for Standardization, "ISO/IEC 27566-1."
[33] Note that "inference" is a technical term in artificial intelligence that more closely approximates what happens in age estimation.
[34] Yoti also lists "Yoti keys" and "Digital ID wallet," but these are mechanisms for avoiding repeating a single age assurance transaction with each new service provider. See Yoti, "Age Verification."

Category	Methods
Age estimation	Facial age estimation
Age inference	Credit card, mobile phone account, social security number, database, email
Age verification	Identity document, electronic ID

Age assurance can take place either on the server (service provider) or on the user's device. The majority of age assurance mandates in the United States and elsewhere make the service provider responsible for providing age assurance, which typically occurs on the server, often using a third-party age verification provider (AVP). The text of the AADC requirements on "covered businesses" appear to apply to the service provider; therefore these comments only consider server-based age assurance.

B. Age Assurance Success and Failure Rates

No age assurance method is capable of providing accurate results for all users. Age estimation techniques inherently have a margin of error and thus cannot accurately distinguish between adults and minors close to the age threshold. Age inference methods return unknown results for users with an insufficient profile in the records being consulted. Methods based on proof of identity are unable to verify the adult status of users without government-issued IDs. Because no single method is sufficient to provide a practical age assurance system, covered operators of online platforms need to offer a variety of methods.

A viable age assurance system should meet two accuracy goals:

- Effectively exclude users under the threshold age (minimize the false accept rate).[35]
- Effectively allow adults to demonstrate that they are above the threshold age (minimize the false reject rate).

There is an inherent tension between these goals, and between the *accuracy* of an age assurance system and the *availability* of the online platform (or certain features of the platform) to the user population. The more stringent requirements are applied for adults to prove their eligibility (thus reducing the false accept rate), the greater the number of adults who will be incorrectly excluded (increasing the false reject rate).

[35] The statistics and testing literature uses a number of terms for error rates, including sensitivity versus specificity, false positive versus false negative, and type I versus type II errors. These can often be hard to interpret because of confusion about whether a "positive" result results in acceptance or rejection. Here we use the terms "false reject" and "false accept" for clarity.

In an age assurance system designed to maximize accurate age estimation, it is important for the "success" condition to include only those instances when the system delivers correct answers. Whether the system returns an inconclusive age assurance outcome or a false reject, the user should have an opportunity to try again with a secondary age assurance method provided by the online platform. With the exception of the situation where a minor presents a government-issued ID for age-proofing, age assurance methods cannot provide a definitive answer that a user is under 18. In most common use cases arising under the regulations, we do not expect minors to present identification to prove that they are under 18, because they are likely to be defaulted into the minor-specific experience anyway. As a result, users who are rejected by one method should not be rejected entirely, but instead need to be offered the opportunity to demonstrate their age via another method. The overall failure rate of an age assurance system is defined by the number of users who are incorrectly classified, whether that incorrect classification is a result of an inconclusive age assurance outcome or of incorrect results.

Any rules specifying maximum false accept rates should also specify maximum false reject rates. Service providers need to balance access with the cost and operational complexity of offering multiple methods and supporting users through a waterfall when individual methods do not work for them. It should not be assumed that compliance with the rules will naturally incentivize all service providers to make sufficiently accurate age assurance available, and specifying only maximum false accept rates risks deployment of methods with high false reject rates. Rules should make clear that service providers have a responsibility to provide sufficiently accurate age assurance to all users who wish to prove that they are adults, rather than rejecting those for whom it is inconvenient or costly to determine their age.

C. Privacy

Most age assurance systems share enough information with the evaluator (typically the AVP) to allow them to determine the user's actual identity. This includes:

- The user's actual name (as on a government ID)
- Some other form of personal information such as an email address, phone number, or social security number.
- The user's face

The first two of these can be mapped directly to the user's identity. The user's face can be used with facial recognition systems to identify the user.

In these designs, the server learns (1) the user's identity and (2) the service provider that they are trying to access. The user's privacy exposure is entirely dependent on administrative and policy controls; in principle the server can retain the user's identity and/or distribute or sell it. If the data is retained, there is an additional risk of disclosure in a subsequent data breach, as has already happened in several

cases where services required users to provide their identities.[36] Depending on the jurisdiction, there may be laws or regulations restricting the use of this information, but the user is unable to determine that the server is complying with these or with its own privacy policy.

In order to protect user privacy, age assurance mandates should at minimum require that the operator delete user information after the age assurance process. While this is a good requirement, it is inherently difficult for the user to verify, and requires users to trust that the AVP is correctly implementing its data protection measures, which does not always happen.[37] Where possible, it is better to use technical controls, which do not require the user to trust the covered operator.

In the context of server-based age assurance, the strongest technical protections are provided by zero-knowledge proofs (ZKPs) of age, which allow a user to demonstrate their age eligibility without disclosing any other information about themselves, even including their precise age or birthday. We recommend that any rule require service providers to provide a ZKP-based age assurance method once technically feasible, specifically once one or more of the mobile operating system vendors with the highest market penetration in Vermont provide a ZKP-based age assurance method that implements a publicly available ZKP technical specification and age assurance protocol.

D. Transparency

Any new rule should require age assurance methods be certified by an accredited provider. This is an important provision, both for ensuring that these methods perform according to the accuracy minimums and for providing accountability to an independent third party and to the AGO about the performance of age assurance methods. We recommend that reports be required to contain the following:

- The specific configuration that was used to test the age assurance method, such as the challenge age for facial age estimation.
- A precise description of the test data.
- The overall accuracy of the collection of offered methods, where acceptance by any of the methods is considered acceptance. This allows for the determination of the overall effectiveness of the covered operator's system.

In general, the certification reports should include enough information to enable independent replication of the claimed results.

[36] Chia, "ID photos of 70,000 users may have been leaked, Discord says"; Wakefield, "My ex stalked me, so I joined a 'dating safety' app. Then my address was leaked."
[37] Age Check Certification Scheme, "Age Assurance Technology Trial," 108-109; Chia, "ID photos of 70,000 users may have been leaked, Discord says."

In addition, certification reports should be required to be public. At present, public information about how age assurance methods work is limited, and very few of the public claims made by corporations about the accuracy and effectiveness of age assurance systems can be independently verified. The promulgation of the AGO's rules provide a unique opportunity to bring increased transparency to this significant change in how users access online services.

Not only would this allow for public evaluation of the results, it will create additional incentives for service providers to continually invest in robust and privacy-protective age assurance, since their own certification reports would be publicly comparable with their competitors' reports.

Bibliography

Age Check Certification Scheme. "Age Assurance Technology Trial: Part C Age Verification." Australia Department of Infrastructure, Transport, Regional Development, Communications, Sports and the Arts, August 2025. https://www.infrastructure.gov.au/sites/default/files/documents/aatt_part_c_digital.pdf.

Allcott, Hunt, Matthew Gentzkow, & Lena Song. "Digital Addiction." *American Economic Review* 112, no. 7 (March 7, 2022): 2424-63. https://web.stanford.edu/~gentzkow/research/DigitalAddiction.pdf.

Alizadeh, Meysam, Emma Hoes, and Fabrizio Gilardi. "Tokenization of social media engagements increases the sharing of false (and other) news but penalization moderates it." *Science Reports* 13 (2023). https://doi.org/10.1038/s41598-023-40716-2.

Altuwairiqi, Majid, Emily Arden-Close, Elvira Bolat, Laura Renshaw-Vuillier, and Paian Ali. "When People Are Problematically Attached to Social Media: How Would the Design Matter?" In *2019 IEEE International Conference on Systems, Man and Cybernetics*, 4211–4218. 2019. https://eprints.bournemouth.ac.uk/32619/1/Majid-IEEE-SMC-2019-Camera-Ready%5B1%5D.pdf

Alutaybi, Aarif, John McAlaney, Angelos Stefanidis, Keith Phalp, and Raian Ali. "Designing social networks to combat fear of missing out." In *Proceedings of the 32nd International BCS Human Computer Interaction Conference*. HCI '18, 2018. https://dl.acm.org/doi/10.14236/ewic/HCI2018.80.

American Psychological Association. "Potential Risks of Content, Features, and Functions: A Closer Look at the Science of How Social Media Affects Youth." April 2024. https://www.apa.org/topics/social-media-internet/youth-social-media-2024.

Bernstein, Gaia. *Unwired: Gaining Control over Addictive Technologies*. Cambridge University Press, 2023.

Burhan, Rasan, and Jalal Moradzadeh. “Neurotransmitter Dopamine (DA) and its Role in the Development of Social Media Addiction.” *Journal of Neurology & Neurophysiology* 11, no. 7 (2020). https://www.iomcworld.org/open-access/neurotransmitter-dopamine-da-and-its-role-in-the-development-of-social-media-addiction.pdf.

Brown, Lorna, and Daria J. Kuss. “Fear of Missing Out, Mental Wellbeing, and Social Connectedness: A Seven-Day Social Media Abstinence Trial.” *International Journal of Environmental Research and Public Health* 17, no. 12 (2020). https://pmc.ncbi.nlm.nih.gov/articles/PMC7345987/.

Chaudhary, Akash, Jaivrat Saroha, Kyzyl Monteiro, Angus G. Forbes, and Aman Parnami. “‘Are You Still Watching?’: Exploring Unintended User Behaviors and Dark Patterns on Video Streaming Platforms.” In *Proceedings of the 2022 ACM Designing Interactive Systems Conference*, 776-791. DIS ‘22, 2022. https://dl.acm.org/doi/10.1145/3532106.3533562.

Chia, Osmond. “ID photos of 70,000 users may have been leaked, Discord says.” *BBC*, October 9, 2025. https://www.bbc.com/news/articles/c8jmzd972leo.

Cho, Hyusung, DaEun Choi, Donghwi Kim, Wan Ju Kang, Eun Kyoung Choe, and Sung-Ju Lee. “Reflect, not Regret: Understanding Regretful Smartphone Use with App Feature-Level Analysis.” Proceedings of the ACM on Human-Computer Interaction 5, no. CSCW2. (2021): 1-36. https://dl.acm.org/doi/10.1145/3479600.

Fitz, Nicholas, Kostadin Kushlev, Ranjan Jagannathan Terrel Lewis, Devang Paliwal, and Dan Ariely. “Batching smartphone notifications can improve well-being.*” Computers in Human Behavior* 101 (2019): 84-94. https://www.sciencedirect.com/science/article/abs/pii/S0747563219302596.

Griffiths, Mark D. “Adolescent social networking: how do social media operators facilitate habitual use?” *Education and Health* 36, no. 3 (2018): 66-69. https://sheu.org.uk/sheux/EH/eh363mdg.pdf.

Hiniker, Alexis, Sharon S. Heung, Sungsoo Hong, and Julie A. Kientz. “Coco’s Videos: An empirical investigation of video-player design features and children's media use.” In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–13. CHI ‘18, 2018. https://dl.acm.org/doi/10.1145/3173574.3173828.

International Organization for Standardization. “ISO/IEC 27566.” December 2025. https://www.iso.org/standard/88143.html.

Langvardt, Kyle. “Regulating Habit-Forming Technology.” Fordham Law Review 88, no. 1 (2019). https://ir.lawnet.fordham.edu/flr/vol88/iss1/4.

Lawrence, Matthew B. “Public Health Law's Digital Frontier: Addictive Design, Section 230, and the Freedom of Speech.” *Journal of Free Speech Law* 4 (2023). https://scholarlycommons.law.emory.edu/faculty-articles/247/.

Lukoff, Kai, Ulrik Lyngs, Hmanshu Zade, et al. “How the Design of YouTube Influences User Sense of Agency.” In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1-17. CHI ‘21, 2021. https://dl.acm.org/doi/10.1145/3411764.3445467.

Natarajan, Nikhila. “Do They Stop? How Do They Stop? Why Do They Stop? Whether, How, and Why Teens Insert ‘Frictions’ into Social Media’s Infinite Scroll.” *International Journal of Communication* 18 (2024): 1956-1975. https://ijoc.org/index.php/ijoc/article/view/21618.

Office of Minnesota Attorney General. “Minnesota Attorney General’s Report on Emerging Technology and Its Effects on Youth Well-Being.” February 2024. https://www.ag.state.mn.us/Office/Reports/EmergingTechnology.pdf.

Office of the Surgeon General. “Social Media and Youth Mental Health: The U.S. Surgeon General’s Advisory.” Publications and Reports of the Surgeon General. US Department of Health and Human Services, 2023. http://www.ncbi.nlm.nih.gov/books/NBK594761/.

Park, Joohye, and Yoonhyuk Jung. “Unveiling the dynamics of binge-scrolling: A comprehensive analysis of short-form video consumption using a Stimulus-Organism-Response model.” *Telematics and Informatics* 95 (2024). https://www.sciencedirect.com/science/article/pii/S0736585324001047.

Qin, Yao, Alessandro Muesetti, and Bahiyah Omar. “Flow Experience Is a Key Factor in the Likelihood of Adolescents’ Problematic TikTok Use: The Moderating Role of Active Parental Mediation.” I*nternational Journal of Environmental Research and Public Health* 20, no. 3 (2023). https://www.mdpi.com/1660-4601/20/3/2089.

Rixen, Jan Ole, Luca-Maxim Meinhardt, Michael Glöckler, et al. “The Loop and Reasons to Break It: Investigating Infinite Scrolling Behaviour in Social Media Applications and Reasons to Stop.” *Proceedings of the ACM on Human-Computer Interaction* 7, no. MHCI (2023): 1-22. https://dl.acm.org/doi/10.1145/3604275.

Roberts, James A., and Meredith E. David. “Instagram and Tiktok Flow States and Their Association with Psychological Well-Being.” *Cyberpsychology, Behavior, and Social Networking* 26, no. 2 (2023): 80–89. https://www.newswise.com/pdf_docs/16835673808410_Instagram%20and%20TikTok%20Flow%20States%20and%20Their%20Association%20with%20Pyschological%20Well-Being.pdf.

Roffarello, Alberto Monge, and Luigi De Russis. “Towards Understanding the Dark Patterns That Steal Our Attention.” In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, 1–7. CHI EA ‘22, 2022. https://doi.org/10.1145/3491101.3519829.

Salerno, Laura, Lucia Fortunato, Vivia Ostwald, Arianna Muscolino, and Gianluca Lo Colo. “Social support and social comparison tendencies predict trajectories of adolescents’ problematic social

media use: A longitudinal study." *PLoS One* 20, no. 6 (2025): e0323320. https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0323320.

Salo, Markus, Henri Pirkkalainen, and Tiina Koskelainen. "Technostress and social networking services: Explaining users' concentration, sleep, identity, and social relation problems." *Information Systems Journal* 29, no. 2 (2019): 408–435. https://onlinelibrary.wiley.com/doi/10.1111/isj.12213.

Schaffner, Brennan, Neha A. Lingareddy, and Marshini Chetty. "Understanding Account Deletion and Relevant Dark Patterns on Social Media." *Proceedings of the ACM on Human-Compatible Interaction* 6, no. CSCW2 (2022): 1-43. https://dl.acm.org/doi/10.1145/3555142.

Schaffner, Brennan, Yaretzi Ulloa, Riya Sahni, et al. "An Experimental Study of Netflix Use and the Effects of Autoplay on Watching Behaviors." *Proceedings of the ACM on Human-Computer Interaction* 9, no. 2 (2025): 1-22. https://dl.acm.org/doi/10.1145/3710928.

Seaborn, Katie, and Deborah I. Fels. "Gamification in theory and action: A survey.' *International Journal of Human-Computer Studies* 74 (2015): 14-31. https://doi.org/10.1016/j.ijhcs.2014.09.006.

Stevic, Anja, Desiree Schmuck, Marina F. Thomas, Kathrin Karsay, and Jorg Matthes. "Distracted children? Nighttime smartphone use, children's attentional problems, and school performance over time." *The Journal of Early Adolescence* 44, no. 2 (2024): 223–249. https://journals.sagepub.com/doi/10.1177/02724316231164734.

Suh, Kil-Soo, Hongki Kim, and Eung Kyo Suh. "What If Your Avatar Looks Like You? Dual-Congruity Perspectives for Avatar Use." *MIS Quarterly* 35, no. 3 (2011): 711–729. https://doi.org/10.2307/23042805.

United States District Court for the Northern District of California. "In re Soc. Media Adolescent Addiction/Personal Injury Products Liability Litigation: Plaintiff's Amended Master Complaint (Personal Injury)." December 15, 2023. https://www.motleyrice.com/sites/default/files/documents/social_media_addiction-redacted_master_complaint.pdf.

Wakefield, Jacqui. "My ex stalked me, so I joined a 'dating safety' app. Then my address was leaked." *BBC*, August 22, 2025. https://www.bbc.com/news/articles/ce87rer52k3o.

Wansink, Brian, James E. Painer, and Jill North. "Bottomless Bowls: Why Visual Cues of Portion Size May Influence Intake." *Obesity* 13, no. 1 (2005): 93-100. https://onlinelibrary.wiley.com/doi/10.1038/oby.2005.12.

Yoti. "Age Verification." Accessed January 13, 2025. https://www.yoti.com/business/age-verification/.

Zeiler, M.D. “Fixed-interval behavior: effects of percentage reinforcement.” *Journal of the Experimental Analysis of Behavior* 17, no. 2 (1972): 177-189. https://pmc.ncbi.nlm.nih.gov/articles/PMC1333957/pdf/jeabehav00131-0041.pdf.

Bambara, Anthony

Subject: RE: Age-Appropriate Design Comments

From: avi <zimetavi@gmail.com>
Sent: Wednesday, September 9, 2026 11:52 AM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: Age-Appropriate Design Comments

Some people who received this message don't often get email from zimetavi@gmail.com. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Hello,

I was at the Sep 9 public hearing and wanted to share my thoughts and raise some questions on this subject. I am far from an expert, but I have had and heard bad experiences with age verification with Discord, Twitter, and particularly in Europe.

I strongly support policies that protect youth from addictive features on apps and social media, and protect their data privacy.
I also support the concern taken to verify a user's age in a way that protects their privacy, however, this is a difficult and evolving problem.

- What are the legal repercussions for a business misusing or leaking user data, beyond a fine?
- Could there be legal support from the state for youth affected by data privacy breaches?
- Will there be state IT support for businesses to protect their data from breaches?
- How will businesses and the state decide what content and features should be protected for the youth, and can it be assured these decisions are not affected by partisan politics and religion?
- How can we assure that youth voices are not censored online? For example, if they have limited posting/visibility on social media.
- Will better data privacy/segregation and not subverting autonomy (like for gambling, sports betting) be expanded to all Vermonters, including adults?
- Will there be ruling to prevent a business from intentionally limiting a user's account features during a pending age verification response period as a means to temporarily ban the account? For adults and minors.

- Will there be public knowledge of the covered businesses, and does this list include popular social media companies run from other states or countries?
- Will the rules prevent or permit invasive monitoring for the purpose of crime prevention?
- I want to mention that my least favorite method of creating "safe" online accounts as a minor is requiring the linking of a parental account. I also strongly dislike any ID uploads or facial verification.

Thanks,
Avi Zimet

Bambara, Anthony

Subject: RE: Technical Input — Vermont Age-Appropriate Design Code | Age Assurance, Interoperability & Verifiable Youth-Safety Controls

From: Ashraf Abdala | CEO, CIVITERA <ceo@civitera.ai>
Sent: Saturday, September 5, 2026 1:42 AM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: Technical Input — Vermont Age-Appropriate Design Code | Age Assurance, Interoperability & Verifiable Youth-Safety Controls

Some people who received this message don't often get email from ceo@civitera.ai. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Dear Attorney General Clark and Vermont Age-Appropriate Design Code Rulemaking Team,

I am Ashraf Izeldin A.E Abdala, Founder & CEO of CIVITERA GOVTECH INC.

I am writing in connection with the Vermont Attorney General's rulemaking under the Vermont Age-Appropriate Design Code and the Office's request for technology standards, industry information, data, and analysis relevant to protecting minors in digital products and services.

CIVITERA GOVTECH INC. has developed a portfolio of U.S. patent-pending technologies addressing technical aspects of youth-safety governance and digital-platform compliance.

The architectures address areas including age- and beneficiary-aware controls, privacy-conscious age and beneficiary determination, cumulative digital-use governance, cross-platform coordination, circumvention resistance, jurisdiction-aware policy execution, feature-level enforcement, and generation of verifiable compliance evidence for independent oversight and audit.

Several technical questions raised by Vermont's rulemaking closely intersect with this work, including how digital services can:

• determine whether a user is a minor using technically feasible and privacy-conscious methods;

• support review or correction where an age designation may be inaccurate;

• reduce unnecessary collection or exposure of age-assurance data;

• evaluate the effectiveness of age-assurance methods rather than relying solely on their nominal implementation;

• support interoperable approaches to age assurance without requiring unnecessary disclosure of identity;

• resist circumvention involving multiple accounts, devices, services, or inconsistent age representations;

• translate jurisdiction-specific youth-safety requirements into enforceable feature-level controls; and

• generate verifiable evidence showing whether required safeguards actually operated.

There is also a broader interoperability challenge.

Children may move among social-media, gaming, messaging, video, AI-enabled, and other digital environments while each service independently determines age or beneficiary status, applies safeguards, measures usage, detects circumvention, and generates compliance evidence.

This fragmentation can create gaps involving cumulative digital use, inconsistent age classifications, repeated age-assurance processes, cross-service circumvention, and limited independent verification of whether protections operated consistently.

We would welcome the opportunity to provide the Vermont Attorney General's Office with a concise, non-confidential technical briefing or technical submission addressing these implementation questions.

Our purpose at this stage is not to advocate for a particular commercial product or policy outcome, interfere with pending litigation or enforcement, seek non-public information, or disclose confidential patent claims.

Rather, we would like to determine whether technical concepts from our work could provide useful input to Vermont's consideration of commercially reasonable, technically feasible, privacy-conscious, interoperable, and independently verifiable approaches to protecting minors.

If useful to the rulemaking team, we can organize a subsequent non-confidential technical submission around specific implementation questions, architecture patterns, verification mechanisms, interoperability considerations, and safeguards for age-assurance data.

If another attorney, technologist, policy team, or rulemaking personnel within the Office is responsible for technical submissions of this nature, I would greatly appreciate it if this communication could be forwarded accordingly or if you could advise us of the appropriate contact.

Thank you for your consideration.

Best regards,

Ashraf Izeldin A.E Abdala
Founder & CEO
CIVITERA GOVTECH INC.
ceo@civitera.ai
www.civitera.ai

Bambara, Anthony

Subject: Technical Comments - Vermont Age-Appropriate Design Code Rulemaking - CIVITERA GOVTECH INC.
Attachments: CIVITERA_Vermont_AADC_Technical_Comments_v1.0.pdf

---

From: Ashraf Abdala | CEO, CIVITERA <ceo@civitera.ai>
Sent: Saturday, September 5, 2026 8:39 AM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: Technical Comments - Vermont Age-Appropriate Design Code Rulemaking - CIVITERA GOVTECH INC.

Some people who received this message don't often get email from ceo@civitera.ai. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Dear Vermont Attorney General's Office,

On behalf of CIVITERA GOVTECH INC., I am submitting the attached non-confidential technical comments concerning the Vermont Age-Appropriate Design Code rulemaking.

The submission focuses on privacy-preserving age assurance, review and correction processes, interoperability, compulsive-use design practices, circumvention resilience, feature-level safeguards, and privacy-minimized technical evidence for evaluating whether material protections operate as intended.

The comments are intended as a technology-neutral technical contribution to the rulemaking process. They do not contain confidential patent claims or proprietary implementation details.

Please include the attached submission in the rulemaking record.

Respectfully,

Ashraf Izeldin A.E Abdala
Founder & CEO
CIVITERA GOVTECH INC.
ceo@civitera.ai
www.civitera.ai

CIVITERA

CIVITERA GOVTECH INC.

Technical Comments on the Vermont Age-Appropriate Design Code Rulemaking

Privacy-Preserving, Circumvention-Resistant, and Verifiable Digital Protections for Minors

NON-CONFIDENTIAL TECHNICAL SUBMISSION

September 2026

Submitted by
Ashraf Izeldin A.E Abdala
Founder & CEO
CIVITERA GOVTECH INC.
ceo@civitera.ai | www.civitera.ai

Public-record safe. No confidential patent claims or proprietary implementation details included.

Executive Summary

CIVITERA GOVTECH INC. respectfully submits these non-confidential technical comments concerning the Vermont Attorney General's rulemaking under the Vermont Age-Appropriate Design Code (AADC). The comments focus on the two rulemaking subjects identified by the Attorney General: (1) data-processing or design practices that lead to compulsive use or subvert or impair user autonomy, decision making, or choice; and (2) commercially reasonable, technically feasible, privacy-minded age-assurance methods, including review processes, interoperability, and additional privacy protections.

The central recommendation is to distinguish the existence of a protective control from the effective operation of that control. A platform may implement an age-assurance mechanism, time limit, notification restriction, parental setting, or other safeguard without establishing that the safeguard operates as represented, remains resistant to reasonably foreseeable circumvention, minimizes unnecessary personal-data processing, and can be independently evaluated.

CIVITERA recommends a technology-neutral implementation model in which age assurance is an input to a continuing protection process rather than the endpoint of compliance. The model should preserve privacy and accessibility, permit multiple assurance methods, support correction of erroneous age designations, focus compulsive-use analysis on system and design behavior rather than media viewpoint or content, and support privacy-minimized evidence sufficient to evaluate material safeguards.

Core principle: Age assurance should be treated as a privacy-limited input to an ongoing protective-control process, not as the endpoint of compliance.

1. Purpose, Scope, and Rulemaking Fit

These comments are offered as a technical contribution. They do not request that Vermont mandate a CIVITERA product, patent, proprietary implementation, or commercial provider. They intentionally omit confidential implementation details, unpublished claim language, proprietary algorithms, thresholds, source code, and other non-public intellectual property.

The Vermont Attorney General is soliciting comments, data, research, technology standards, industry information, examples, and analysis to assist with rules under 9 V.S.A. §§ 2449f and 2449g. CIVITERA therefore confines its recommendations primarily to those delegated subjects: compulsive-use and autonomy-related design practices, and age-assurance privacy and implementation.

2. A Core Regulatory Distinction: Control Presence vs. Control Effectiveness.

A material technical distinction exists between control presence and control effectiveness. A service can show that a daily-use limit, age-assurance process, notification restriction, or other safeguard exists without showing that the safeguard actually operated under the conditions for which it was designed.

For material safeguards, Vermont should consider whether a regulated entity can demonstrate, using proportionate and privacy-preserving evidence, which policy applied, which control was expected, whether it executed, and whether reasonably foreseeable bypass conditions materially defeated it. The rule need not prescribe a proprietary measurement formula; it can instead define the properties that a credible effectiveness assessment should address.

3. Age Assurance Is an Input, Not the Endpoint

Age assurance is necessary to the AADC framework, but an age designation alone does not determine the appropriate protection. Once an age range is established, a covered business still must apply the legal and technical consequences associated with that designation.

CIVITERA recommends that Vermont avoid treating completion of an age-assurance step as a proxy for substantive safety compliance. The age-range result should be treated as a narrowly scoped input into subsequent policy and feature behavior, consistent with the statutory limits on collection, use, combination, disclosure, and retention of age-assurance data.

4. Privacy-Preserving, Vendor-Neutral Age Assurance

Vermont law requires privacy and accessibility to be prioritized over accuracy and directs the Attorney General to consider cost, effectiveness, safety, utility, user experience, transparency, previously collected data, interoperability, and multiple assurance options. A rule should therefore remain technology-neutral and avoid creating a de facto requirement that every service collect identity documents, biometrics, or equivalent high-risk data.

Where technically feasible, the architecture should favor the minimum assertion necessary for the legal purpose. A service may need an age range or protected-status result; it may not need the underlying identity document, full birth date, facial template, or unrelated identity attributes. Age-assurance data should remain purpose-limited and separated from unrelated commercial profiling or behavioral enrichment.

5. Review, Correction, and Recovery from Erroneous Age Designations

An age-assurance system must include a usable correction path. Vermont law expressly requires a review process allowing users to appeal an age determination, and the rulemaking must describe appropriate review processes.

A technology-neutral review flow can be expressed as: Age Determination -> Notice or Result -> User Challenge -> Alternative Approved Method or Reassessment -> Correction -> Operational Update. The review process should be accessible, proportionate, timely, and designed so that a successful appeal corrects the operational designation without preserving unnecessary underlying identity evidence. The system should also prevent an appeal process from becoming a dark pattern that makes correction practically unavailable.

6. Material Uncertainty About the Protected User

Account ownership and actual use are not always identical. Shared devices, family accounts, delegated access, or other ordinary arrangements can create uncertainty about whether the registered account holder is the person receiving a feature.

CIVITERA does not recommend persistent identity resolution or continuous biometric surveillance. Instead, protective controls should be capable of accounting for material uncertainty, where relevant and legally permitted, without requiring a universal identity layer. The objective is to avoid designing safeguards on the categorical assumption that account registration always establishes the protected user.

7. Feature-Level and Capability-Aware Protection

Digital services contain capabilities with materially different risk characteristics. A binary account-wide model can be unnecessarily coarse. A technology-neutral rule can recognize that safeguards may operate at the level of a feature or capability - for example, notifications, private messaging, live interaction, recommendation behavior, location functionality, payments, or AI-mediated interaction - without prescribing the specific outcome for every service.

This approach also aligns with the AADC's focus on an online service, product, or feature. It permits proportionality: lower-risk functionality need not automatically be disabled merely because a higher-risk capability requires stronger safeguards.

8. Compulsive Use: Focus on System and Design Behavior, Not Media Viewpoint

Vermont's AADC directs the Attorney General to prohibit data-processing or design practices that lead to compulsive use or subvert or impair autonomy, decision making, or choice. At the same time, the statute provides that the content of media viewed by a covered minor does not itself establish compulsive use and does not require a business to prevent access to a piece or category of media.

CIVITERA therefore recommends that compulsive-use rules focus on system behavior and interaction design: engagement loops, autoplay or equivalent continuation mechanics, notification patterns, recommendation mechanics, friction or absence of friction, session design, reward structures, and other processing or design practices that can materially affect

autonomy. The framework should not be interpreted as a recommendation to regulate the viewpoint or substantive content of media.

9. Circumvention Resilience

A safeguard that can be trivially bypassed may exist formally while failing operationally. Reasonably foreseeable bypass conditions can include changes in account, access channel, device, declared age, or functionally equivalent feature.

CIVITERA recommends a proportional principle: material safeguards should be designed and evaluated with reasonably foreseeable circumvention in mind, while any detection or response mechanism remains constrained by necessity, privacy, data minimization, accuracy, security, and accessibility. Circumvention resistance and privacy should be treated as simultaneous engineering requirements, not opposing objectives.

10. Interoperability Without Cross-Service Behavioral Tracking

The statute expressly directs the Attorney General to consider the efficacy of interoperable age-assurance methods. CIVITERA recommends that interoperability be evaluated first at the narrow age-assurance assertion layer: whether a reliable, privacy-preserving age-range or eligibility assertion can reduce repeated collection of sensitive identity evidence.

Interoperability should not become a mandate for cross-service behavioral identity linkage or a universal child-tracking identifier. Where an interoperable assertion is used, the receiving service should obtain only the minimum information necessary for the applicable purpose, subject to the statute's use, combination, disclosure, and deletion restrictions.

11. Measuring Compulsive-Use Interventions

A nominal safeguard and an effective safeguard are not necessarily equivalent. For example, a pause, notification restriction, or session-related intervention can be configured yet have little practical effect if it is easily bypassed or immediately displaced by equivalent functionality.

Vermont can preserve implementation flexibility by requiring an appropriate technical basis for evaluating whether material interventions operate as represented, rather than prescribing a single metric. Relevant evaluation may consider the intervention, its observable technical outcome, material bypass conditions, and whether subsequent product changes degrade the safeguard. Any measurement should minimize personal data and avoid converting safety evaluation into continuous surveillance.

12. AI-Mediated Features and Emerging Technology

The Attorney General must periodically review and update the rules to keep pace with emerging technology. A capability-oriented framework is therefore preferable to one tied only to current product labels.

AI-mediated functionality can combine conversational interaction, generated recommendations, persistent memory, synthetic personas, proactive prompts, or agent-like behavior. The relevant regulatory question should remain what capability is delivered, what data processing or design behavior is involved, and whether the applicable protection operates. This permits the framework to remain useful as conventional interfaces evolve.

13. From Rule to Observable Technical Control

A recurring implementation problem is the distance between a legal requirement and observable system behavior. A technology-neutral compliance lifecycle can be represented as: Legal Requirement -> Versioned Policy -> Applicable Feature/Context -> Technical Control -> Outcome -> Privacy-Minimized Evidence -> Authorized Review.

This does not imply government operation of platform systems or access to private communications. The purpose is traceability: where a material safeguard is required, an authorized reviewer should be able to determine what rule or policy applied, what control was expected, whether it operated, and what evidence supports that conclusion.

14. Privacy-Minimized Evidence and Independent Verification

Compliance evidence creates its own privacy risk. Evidence designed to demonstrate youth-safety compliance should not become an unnecessary repository of children's identity documents, private communications, or complete behavioral histories.

CIVITERA recommends privacy-minimized evidence: retain only what is reasonably necessary to demonstrate the relevant compliance condition. Depending on the requirement, this may include a policy version, relevant protection category or age range, control expected, control outcome, time or applicable period, and integrity reference - without retaining the raw data used to make the underlying age-assurance determination.

For material safeguards, evidence should be sufficiently reliable to permit authorized independent evaluation or reconstruction. The goal is verifiability without unnecessary surveillance.

15. Recommended Rulemaking Principles

1. Technology neutrality - define protective outcomes and properties rather than mandating one vendor or technique.

2. Privacy and accessibility first - implement the statutory priority expressly.

3. Data minimization - collect and retain only what is necessary for age assurance and the permitted age-range result.

4. Multiple assurance options - reduce exclusion and single-point dependence where feasible.

5. Meaningful appeal - provide an accessible correction process with alternative reassessment paths.

6. Age assurance is an input - do not equate an age check with substantive safety compliance.

7. Capability-aware safeguards - allow proportional controls at the relevant feature level.

8. System-behavior focus - address compulsive design and processing practices without regulating media viewpoint.

9. Circumvention resilience - consider reasonably foreseeable bypasses while preserving privacy and proportionality.

10. Narrow interoperability - prioritize privacy-preserving age assertions rather than cross-service behavioral tracking.

11. Effectiveness and verifiability - material safeguards should be capable of objective evaluation.

12. Emerging-technology resilience - write rules around capabilities and design effects so they can adapt to AI-mediated services.

Conclusion

CIVITERA GOVTECH INC. respectfully encourages Vermont to frame the AADC rules around a complete technical question: Was the appropriate protection applied under the relevant conditions, did it operate as represented, were unnecessary personal data minimized, could an erroneous age designation be corrected, and can material safeguards be evaluated without creating a new surveillance system?

A technology-neutral framework built around privacy, accessibility, proportionality, effectiveness, correction, circumvention resilience, and verifiability can support stronger protections for minors while allowing covered businesses to adopt improved technologies over time.

CIVITERA GOVTECH INC. would welcome the opportunity to provide additional non-confidential technical information concerning age-assurance architecture, privacy-preserving

interoperability, compulsive-use controls, circumvention resilience, feature-level safeguards, and compliance verification.

Annex A - Vermont Rulemaking-to-Architecture Matrix

Rulemaking issue	Technical concern	Recommended principle	Evaluation objective
Compulsive use	Nominal safeguard may not change system behavior	Outcome-oriented, design-behavior analysis	Determine whether material intervention operated as represented
Age assurance	Overcollection or single-method dependence	Vendor-neutral, privacy-first, multiple options	Determine age range while minimizing underlying data
Appeals	Incorrect designation becomes persistent	Accessible reassessment and correction	Verify timely operational correction
Privacy	Age evidence reused or combined	Strict purpose limitation and deletion	Verify minimization, separation, and retention controls
Interoperability	Repeated identity collection or tracking	Narrow age-assertion interoperability	Reduce repeated collection without behavioral linkage
Feature risk	Account-wide controls may be disproportionate	Capability-aware safeguards	Verify action at the relevant feature
Circumvention	Easy bypass undermines protection	Proportionate resilience	Evaluate material bypass conditions
Emerging AI	New interfaces escape legacy categories	Capability-oriented governance	Maintain applicability as technology changes
Verification	Provider assertion is difficult to test	Privacy-minimized evidence	Support authorized independent evaluation

Annex B - Illustrative Reference Architecture

AGE-RANGE / ELIGIBILITY ASSERTION

↓

PRIVACY-LIMITED ASSURANCE STATE

↓

APPLICABLE PROTECTION POLICY

↓

FEATURE / CONTEXT / DESIGN CONDITION

↓

PROPORTIONATE TECHNICAL CONTROL

↓

OUTCOME / EFFECTIVENESS OBSERVATION

↓

PRIVACY-MINIMIZED EVIDENCE

↓

AUTHORIZED INDEPENDENT EVALUATION

Illustrative only. This architecture does not prescribe a specific vendor, algorithm, data model, identity provider, or proprietary implementation.

Annex C - Selected Public Authorities

Office of the Vermont Attorney General, Vermont Age-Appropriate Design Code Rulemaking (accessed September 5, 2026).

9 V.S.A. § 2449f, Prohibited data and design practices (effective January 1, 2027).

9 V.S.A. § 2449g, Age assurance privacy (effective January 1, 2027).

9 V.S.A. § 2449c, Minimum duty of care (effective January 1, 2027).

9 V.S.A. § 2449a, Definitions (effective January 1, 2027).

Official rulemaking page: ago.vermont.gov/vermont-age-appropriate-design-code-rulemaking

Vermont Statutes Online: legislature.vermont.gov/statutes/chapter/09/062

Submission Contact

Ashraf Izeldin A.E Abdala
Founder & CEO
CIVITERA GOVTECH INC.
ceo@civitera.ai
www.civitera.ai

Bambara, Anthony

Subject: CCIA Comments_AGO Age Appropriate Design Code Proposed Regulations

From: Jameson, Sarah <Sarah.Jameson@vermont.gov>
Sent: Monday, September 21, 2026 1:14 PM
To: Bambara, Anthony <Anthony.Bambara@vermont.gov>
Subject: FW: CCIA Comments_AGO Age Appropriate Design Code Proposed Regulations

Tony, can you please post the attached document on the rulemaking site? Thanks!

From: Kyle Sepe <ksepe@ccianet.org>
Sent: Monday, September 21, 2026 12:25 PM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: CCIA Comments_AGO Age Appropriate Design Code Proposed Regulations

Some people who received this message don't often get email from ksepe@ccianet.org. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

The Computer & Communications Industry Association (CCIA) respectfully submits the attached comments in response to the proposed rules implementing §§ 2449f and 2449g of Act 63 of 2025, the Vermont Age-Appropriate Design Code Act ("VAADCA"). CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.

--

Kyle J. Sepe
State Policy Manager, Northeast Region
ksepe@ccianet.org
M: 908-838-8980

Computer & Communications Industry Association
Open Markets. Open Systems. Open Networks.

ccianet.org | @CCIAnet

September 21, 2026

The Honorable Charity R. Clark
109 State Street
Montpelier, VT 05609

Re: Proposed Rules Implementing §§ 2449f and 2449g of Act 63 (Vermont Age-Appropriate Design Code Act)

Dear Attorney General Clark:

The Computer & Communications Industry Association (CCIA) respectfully submits these comments in response to the proposed rules implementing §§ 2449f[1] and 2449g[2] of Act 63 of 2025, the Vermont Age-Appropriate Design Code Act ("VAADCA").[3] CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[4]

CCIA firmly believes that children are entitled to security and privacy online. Our members have developed settings, safeguards, and parental controls designed to tailor younger users' online experiences to their developmental needs. These include tools that allow parents to set time limits and restrict access to particular services, as well as enhanced privacy protections enabled by default for known child users.[5] This is also why CCIA supports implementing digital citizenship curricula in schools, to not only educate children on proper social media use but also help teach parents how they can use existing mechanisms and tools to protect their children as they see fit.[6]

While CCIA supports the Office of the Attorney General ("AGO's") commitment to protecting minors online, the proposed rules, if implemented, raise significant concerns. In numerous instances, the proposed rules exceed Act 63's scope, introduce novel legal standards not found in the enabling legislation, and contain inconsistencies that will frustrate compliance and undermine the very protections VAADCA seeks to provide. We respectfully urge the AGO to

---

[1] "Prohibited Data and Design Practices" (Regulations Adopted Pursuant to 9 V.S.A. § 2449f), https://ago.vermont.gov/sites/ago/files/2026-07/AADC%20rules/2026.07.08%20-%202449f%20Prohibited%20Data%20and%20Design%20Practices%20-%20FINAL%20DRAFT.pdf.
[2] "Age Assurance Privacy" (Regulations Adopted Pursuant to 9 V.S.A. § 2449g), https://ago.vermont.gov/sites/ago/files/2026-07/AADC%20rules/2026.07.08%20-%202449g%20Age%20Assurance%20Privacy%20-%20FINAL%20DRAFT.pdf.
[3] 9 V.S.A. §§ 2449a–2449h (2025), https://legislature.vermont.gov/Documents/2026/Docs/ACTS/ACT063/ACT063%20As%20Enacted.pdf.
[4] 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. A list of CCIA members is available at https://www.ccianet.org/members.
[5] Competitive Enterprise Inst., *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/ (last updated July 28, 2026).
[6] Jordan Rodell, *Why Implementing Education is a Logical Starting Point for Children's Safety Online*, Disruptive Competition Project (Feb. 7, 2023), https://project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/.

revise the proposed rules to comply with Act 63, align with established legal frameworks, and preserve beneficial uses of data that serve minors' interests. CCIA therefore recommends the revisions detailed in the responses to the questionnaire below:

10. Discuss the relevant factors for assessing what constitutes design practices.

VAADCA authorizes the AGO to regulate design practices "that lead to compulsive use or subvert or impair user autonomy, decision making, or choice."[7] VAADCA further defines "compulsive use" as "the repetitive use of a covered business's service that materially disrupts one or more major life activities of a minor, including sleeping, eating, learning, reading, concentrating, communicating, or working."[8] To avoid legal inconsistency, interpretation of the phrase "subvert or impair user autonomy, decision making, or choice" should match the analogous definition of "dark pattern" in the Vermont Data Privacy and Online Surveillance Act (VDPOSA).[9] VDPOSA uses this terminology only in the consent context.[10] Accordingly, any design feature of a user interface deemed to invalidate user consent, either under VDPOSA or by the Federal Trade Commission, should constitute a "design practice" that the proposed rules may regulate. Designed aspects of online services that do not meet either of these criteria do not fall within VAADCA's scope.

By contrast, the proposed rules define "subvert or impair autonomy" as "practices that interfere with a covered minor's informed decision-making or make disengagement from a service harder."[11] This definition extends far beyond material disruption of major life activities, and contains no connection to the consent context. If this definition is not narrowed as proposed above, it will exceed VAADCA's statutory authority and conflict with the term's common understanding in the privacy context.

11. Discuss businesses to be considered 'covered businesses' for purposes of assessing what would subvert or impair user autonomy, decision making, or choice.

The definition of "covered business" should provide clear, objective criteria that allow businesses to determine whether they are subject to the VAADCA. As the term "reasonably likely to be accessed by a minor" is inherently subjective, the AGO should interpret this term to align with the standard for determining when an online service is "directed to" children under the Children's Online Privacy Protection Act of 1998 ("COPPA"),[12] as VAADCA does.[13] The FTC has already issued extensive guidance to assist businesses in making such determinations.[14]

---

[7] 9 V.S.A. § 2449f(b).
[8] § 2449a(8).
[9] § 2415a(b)(16) (2026), https://legislature.vermont.gov/Documents/2026/Docs/ACTS/ACT145/ACT145%20As%20Enacted.pdf..
[10] § 2415a(b)(7)(C)(iii).
[11] "Prohibited Data and Design Practices" (Regulations Adopted Pursuant to 9 V.S.A § 2449f), 3, https://ago.vermont.gov/sites/ago/files/2026-07/AADC%20rules/2026.07.08%20-%202449f%20Prohibited%20Data%20and%20Design%20Practices%20-%20FINAL%20DRAFT.pdf.
[12] 15 U.S.C. §§ 6501-06 (1998), https://www.law.cornell.edu/uscode/text/15/chapter-91.
[13] 9 V.S.A. § 2449a(26)(A) (2025).
[14] *See, e.g.*, 16 C.F.R. § 312.2.5, https://www.federalregister.gov/d/2025-05904/p-326.

Absent such guidance, businesses will likely be unable to determine in advance whether they must comply with the law.

12. Discuss the types of data processing or design practices that should be considered.

The proposed rules contain numerous conflicts with VAADCA regarding design practices. As noted above, the statute authorizes the AGO only to regulate design practices "that lead to compulsive use or subvert or impair user autonomy, decision making, or choice." However, the proposed data and design practices rules instead aim to regulate "any online service, product, or feature that is used by a covered minor."[15] Only a limited subset of all online services, products, and features used by minors will lead to the outcomes contemplated in VAADCA. CCIA therefore recommends revising the "Applicability" section of the proposed data and design practices rules to match the scope authorized by VAADCA.

The proposed data and design practices rules further exceed the statutory mandate by regulating data that does not qualify as "personal data" under VAADCA. VAADCA defines "personal data" as information "linked or reasonably linkable to an identified or identifiable individual,"[16] and does not regulate the processing of non-personal data. However, the proposed rules define "behavioral data" to include many types of data that are not necessarily "linked or reasonably linkable" to an individual. Online services regularly conduct aggregate analyses of the "clicks, scrolls, dwell time, viewing history, and navigation patterns" of their overall website traffic after de-identifying it. Such data is "behavioral data," but is not "personal data" and thus not within the proposed rules' scope. To avoid scoping in data beyond what the statute authorizes, CCIA recommends removing the definition of "behavioral data" from the proposed rules. If the behavioral data is also personal data, it will still fall within the rules' scope. Definitions and regulations referencing behavioral data should reference personal data instead.

The "behavioral inference" definition should be removed for similar reasons. Furthermore, the term does not appear elsewhere in the proposed rules, and is redundant given the definition of "inferred preferences," which covers substantially similar activities.

Furthermore, the "minimum duty of care" provision also lies outside the AGO's rulemaking authority. While VAADCA creates a "minimum duty of care" for covered businesses who process covered minors' data, it does not authorize the AGO to institute regulations regarding this duty.[17] Again, the AGO's rulemaking authority applies only when "design practices "lead to compulsive use or subvert or impair user autonomy, decision making, or choice," a far narrower set of circumstances. All regulations regarding the minimum duty of care should therefore be removed, as they exceed the authorized scope for the proposed rules.

Likewise, the proposed rules should remove the definition of "heightened risk of harm," as it covers features that are designed to increase minors' engagement generally. Because not all

[15] "Prohibited Data and Design Practices," *supra* note 1, at 1.
[16] 9 V.S.A. § 2449a(21).
[17] § 2449c.

features designed to increase minors' engagement impair user autonomy or choice, this definition broadens the proposed rules' scope beyond what VAADCA authorizes. Compulsive use determines whether the AGO can regulate a design practice, not attempts to increase engagement.

13. Discuss the types of digital products that should be considered in adopting any AADC rules for purposes of assessing an online service, product, or feature.

Assessments of online services, products, and features should be based on their actual knowledge of users' ages, not what they "have reason to know." VAADCA only applies to "a consumer who a covered business actually knows is a minor or labels as a minor pursuant to age assurance methods in rules adopted by the Attorney General."[18] By contrast, the proposed rules "apply where a covered business knows *or has reason to know* that a user is a covered minor,"[19] thus expanding VAADCA's scope from an actual knowledge standard to a constructive knowledge standard.

Besides exceeding statutory authority, the constructive knowledge standard undermines privacy and prevents equitable enforcement. Because no objective standard exists for determining when a controller "has reason to know" a user's age, covered services will be incentivized to verify the ages of all users to mitigate litigation risk, requiring the collection of additional sensitive information from both minors and adults. Furthermore, this standard is unworkable, leaving covered businesses without a reliable way to know if they are complying with the law. This standard creates unpredictable liability, especially if interpreted to include aggregate information about a service's user base rather than user-specific facts.[20]

14. Discuss what should qualify as an exclusion regarding the sale, delivery, or use of a physical product when assessing an online service, product, or feature.

This exclusion should cover all data reasonably necessary for the sale, delivery, or use of physical products. The proposed rules should not extend to addresses, shipping receipts, and other personal information commonly collected to facilitate sales of physical products. Likewise, the rules should not extend to any internal processing of this data or its use in models, nor should they apply to personal data entered into a physical device that will not be collected or processed online. Otherwise, routine information necessary to complete a transaction, deliver a product, provide warranty or customer support, or enable functionality of a physical device could inadvertently bring ordinary commercial activity within rules aimed at online design practices affecting minors.

[18] § 2449a(12).
[19] "Prohibited Data and Design Practices," *supra* note 1, at 1 (emphasis added).
[20] *See also* Jesse Lieberfeld, *Knowledge Standards in Online Safety and Privacy Legislation*, CCIA (Apr. 14, 2026), https://ccianet.org/articles/knowledge-standards-in-online-safety-and-privacy-legislation/.

15. Discuss the types of technical requirements that should be considered in the AADC rulemaking process.

The proposed AADC rules create technical requirements that directly contradict the statutory text. The rules prohibit ranking, selecting, or prioritizing content based on "inferred preferences,"[21] i.e. predictions made using "a covered minor's personal data, behavioral data, prior activity, interactions, or engagement patterns."[22] VAADCA, by contrast, explicitly allows covered businesses to recommend to covered minors "media with similar characteristics as the media they are currently viewing."[23] Implementing that statutory permission may necessarily require a service to draw conclusions about what media a user is likely to find relevant based on the media currently being viewed. Yet the proposed rules disallow these inferences even though VAADCA unambiguously permits them. The prohibition on using "inferred preferences" to rank, select, or prioritize content should therefore be removed so that the proposed rules comply with the statute.

16. Discuss the types of technical or design challenges that may prohibit data processing or design practices of a covered business for purposes of the AADC rulemaking.

Although the proposed rules do not explicitly mandate age verification, businesses nevertheless may need to *determine the age of all users* to ensure that they adhere to the regulations regarding minors. As explained above, this in turn requires using invasive age verification methods that force businesses to collect sensitive personal identifying information about their users.[24] Maintaining user privacy under these conditions can be enormously challenging.[25] A recent Digital Trust & Safety Partnership (DTSP) report found that "[h]ighly accurate age assurance methods may depend on collection of new personal data such as facial imagery or government-issued ID."[26]

Additionally, age estimation software will sometimes classify adults as minors, or vice versa, and does not process all populations with equal accuracy. The National Institute of Standards and Technology (NIST) recently published a report evaluating six software-based age estimation and age verification tools that estimate a person's age based on the physical characteristics evident in a photo of their face.[27] The report notes that facial age estimation accuracy is strongly influenced by algorithm, sex, image quality, region-of-birth, age itself, and

---

[21] "Prohibited Data and Design Practices," *supra* note 1, at 1.
[22] *Id.* at 12.
[23] 9 V.S.A. § 2449f(a)(4)(A)(iii) (2026).
[24] Berin Szóka, *Comments of TechFreedom In the Matter of Children's Online Privacy Protection Rule Proposed Parental Consent Method; Application of the ESRB Group for Approval of Parental Consent Method*, TechFreedom (Aug. 21, 2023), https://techfreedom.org/wp-content/uploads/2023/08/Childrens-Online-Privacy-Protection-Rule-Proposed-Parental-Consent-Method.pdf.
[25] Kate Ruane, *CDT Files Brief in* NetChoice v. Bonta *Highlighting Age Verification Technology Risks* (Feb. 10, 2025), https://cdt.org/insights/cdt-files-brief-in-netchoice-v-bonta-highlighting-age-verification-technology-risks/.
[26] *Age Assurance: Guiding Principles and Best Practices*, DTSP (Sept. 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.
[27] Kayee Hanaoka et al., *Face Analysis Technology Evaluation: Age Estimation and Verification (NIST IR 8525),* Nat'l Inst. Standards & Tech. (May 30, 2024), https://doi.org/10.6028/NIST.IR.8525.

interactions between those factors, with false positive rates varying across demographics, generally being higher in women compared to men. CCIA encourages the AGO to consider the current technological limitations in providing reliably accurate age estimation tools across all demographic groups.

17. Discuss other factors that may be relevant in developing these rules in developing AADC rules.

Besides contradicting VAADCA as noted above, the proposed AADC rules raise serious First Amendment concerns. In 2024, the Supreme Court held in *Moody v. NetChoice LLC* that "regulating the content-moderation policies" of websites "to change the speech that will be displayed there… is a preference" that states "may not impose."[28] However, the proposed AADC rules explicitly regulate such policies to change what speech covered businesses will display. By restricting the methods through which covered services may select, rank, and present protected expression to users, the proposed rules burden editorial choices concerning the presentation of speech and therefore raise serious First Amendment concerns.

Importantly, the proposed rules regulate not only what information covered businesses may *collect*, but also what they may *infer* from information they have already collected. The regulation of inferences is a restriction on thought rather than a restriction on data processing. The Supreme Court has held that the "right to speak" encompasses the right to decide how "the information" one "possesses" "might be used or disseminated."[29] The proposed rules do not allow covered businesses this necessary discretion.

A blanket ban on personalized recommendations for minors is also misguided from a policy standpoint, and will make minors less safe online. Such systems perform many useful functions, including helping users discover relevant information, creators, communities, businesses, and safety resources. Personalized recommendations can also be an important part of trust and safety systems. Services use automated systems to detect spam, scams, abuse, potentially harmful material, and other content that users may not want to encounter. Algorithmic feeds can limit the spread of such harmful content more easily than reverse-chronological feeds.

18. Discuss how covered businesses currently determine age for compliance with other federal and state laws that require it.

COPPA is the main federal law regulating children's online privacy, and applies to providers "with actual knowledge that [personal] information was collected from a child."[30] Covered businesses have many sources of guidance on how to comply with this standard. While COPPA's statutory text does not further define the term "actual knowledge," the Federal Trade Commission (FTC) has issued guidance on this point. According to the FTC, "an operator has actual knowledge of a user's age if the site or service asks for — and receives — information

[28] 144 S. Ct. 2383, 2408 (2024).
[29] *Sorrel v. IMS Health, Inc.*, 564 U.S. 552, 568 (2011) (cleaned up).
[30] 15 U.S.C. § 6501(4)(B) (1998).

from the user that allows it to determine the person's age,"[31] e.g., by asking for a user's date of birth. Actual knowledge can also be satisfied through age-adjacent requests which provide operators with sufficient notice of a user's age. For example, questions that ask an individual's grade in school or what school they attend may satisfy actual knowledge under COPPA. FTC consent decrees have provided further guidance,[32] as have federal courts.[33]

This combination of underlying federal law, regulatory guidance, FTC enforcement actions, and judicial interpretation provides operators with many tools for understanding compliance requirements.[34] Conversely, as noted above, there is no established framework for determining which information a "covered business collects, processes, or infers" would indicate that a user is a minor.

While several states have sought to exceed the self-attestation requirement and institute age verification mandates, courts have been skeptical of their constitutionality. Several federal courts have held that laws requiring age verification and parental consent for social media sites violate the First Amendment's guarantee of free speech. The Supreme Court has repeatedly ruled that the First Amendment applies to teens as well as adults, holding that "[m]inors are entitled to a significant measure of First Amendment protection, and only in relatively narrow and well-defined circumstances may government bar public dissemination of protected materials to them."[35] The Court has further held that "to foreclose access to social media altogether is to prevent the user from engaging in the legitimate exercise of First Amendment rights."[36] Forcing covered operators to adopt age verification contradicts this ruling, foreclosing a wide range of protected speech for a population clearly entitled to access it. Such laws, in the Court's words, "do not enforce parental authority over children's speech . . . ; they impose *governmental* authority, subject only to a parental veto."[37] For these reasons, a wide array of lower courts have held that the First Amendment does not permit states to require age verification or parental consent to access protected speech as well.[38]

Implementing a statewide mandate with similar consequences in Vermont would cause similar constitutional problems. To avoid these problems, the AGO should continue to hold covered operators to the actual knowledge standard set forth in VAADCA.

19. Discuss how effective current federal and state age assurance requirements, such as state gambling laws, are in ensuring age accuracy.

[31] "Children's Online Privacy Protection Rule: Not Just for Kids' Sites," F.T.C. (May 2026), https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-not-just-kids-sites#when
[32] *See, e.g.*, *FTC v. Google*, No. 1:19-cv-02642 (D.D.C. Sept. 4, 2019); *United States v. Musical.ly*, No. 2:19-cv-01439 (C.D. Cal. Mar. 27, 2019).
[33] *See, e.g.*, *New Mexico v. Tiny Lab Prods.*, 457 F. Supp. 3d 1103, 1129 (D.N.M. 2020).
[34] *See also* Lieberfeld, *supra* note 20.
[35] *See, e.g.*, *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 212-13 (1975); *Brown v. Ent. Merchs. Ass'n*, 564 U.S. 786, 794 (2011).
[36] *Packingham v. North Carolina*, 582 U.S. 98, 108 (2017).
[37] *Brown*, 564 U.S. at 795 n. 3.
[38] *See, e.g.*, *NetChoice v. Hilgers*, No. 4:26-CV-3149, 2026 WL 1850018 (D. Neb. June 27, 2026); *NetChoice v. Jones*, 822 F. Supp. 3d 656 (E.D. Va. 2026); *NetChoice v. Murrill*, 812 F. Supp. 3d 594 (M.D. La. 2025); *NetChoice v. Carr*, 789 F. Supp. 3d 1200 (N.D. Ga. 2025); *NetChoice v. Griffin*, No. 23-cv-05105, 2025 WL 978607 (W.D. Ark. Mar. 31, 2025); *NetChoice v. Reyes*, 748 F. Supp. 3d 1105 (D. Utah 2024).

When states attempt to force online service providers to verify users' ages rather than permit age assurance, numerous problems arise. Many users will be above the age threshold but lack the required proof (such as a driver's license). Additionally, age estimation tools like face scans are prone to both false negatives and false positives.[39] Furthermore, similar age restrictions have been only marginally effective, reducing use of the restricted website by only 10-25 percent among the intended groups, with much of the lost traffic redirected to un-gated websites providing similar content.[40] The limited effectiveness of these measures should be weighed against their substantial consequences for privacy, competition, and access to protected speech. CCIA therefore again recommends replacing the "has reason to know" standard with an actual knowledge standard, as mandated by VAADCA.

20. Discuss the important elements of an age assurance method.

Age assurance is a complex topic and there is no unique and generally applicable solution with services opting for different approaches based on factors such as type of service, target audience, calculation and perception of the risks, privacy and security expectations of users, or economic feasibility, among others.[41]

Relying on industry's best practices and examining their accuracy and impact is a necessary first step. Established industry standards can provide great value in implementing the listed principles. Further, there is a need to guarantee operational capacity for adequate enforcement, allowing the industry to layer and combine different approaches when it comes to age assurance, in order to appropriately target the risks within the different parts of an online service.

21. Discuss the key challenges to an effective age assurance method.

Privacy concerns and technological limitations are among the foremost challenges in creating effective age assurance. Demanding precise age verification often requires collecting more sensitive personal data, such as government IDs or facial scans. This creates larger data pools, particularly attractive for malicious actors and which raise significant privacy concerns for all users, including minors themselves. CCIA recommends avoiding requirements that inadvertently lead to greater data collection than necessary.

Additionally, many age assurance technologies are not consistently effective or accurate across all demographics. This leads to high numbers of false positives, potentially denying adults access to legitimate services, and may even enhance discrimination against certain groups. In this context, CCIA warns against relying on technology that is not yet fully mature, which can create more problems than it solves.

---

[39] Hanaoka et al., *supra* note 27. For a summary of recent literature on various age assurance methods, *see* Trevor Wagener, *App Store Age Verification: Popular in Principle, Unworkable in Practice*, CCIA (Oct. 21, 2025), https://ccianet.org/articles/app-store-age-verification-popular-in-principle-unworkable-in-practice/.
[40] *See, e.g.*, Matthew Brown et. al., *Can Online Activity Be Regulated? Evidence from Adult Websites* (Aug. 4, 2026), https://mattbrownecon.github.io/assets/papers/ageverification/ageverification.pdf; Leonardo Bursztyn et al., Why Bans Fail: Tipping Points and Australia's Social Media Ban, U. Chi. (Apr. 27, 2026), https://home.uchicago.edu/bursztyn/WhyBansFail.pdf.
[41] *Age Assurance*, *supra* note 26.

22. List and discuss the types of age-assurance methods that are commercially reasonable and technically feasible.

While more stringent methods will be appropriate in certain circumstances, covered businesses should be given the option to rely on user self-attestation to ensure equitable enforcement. If self-attestation is not an option, determining whether a given age assurance method is "commercially reasonable and technically feasible" will almost certainly require case-by-case evaluations of granular details about digital services' designs, user behavior, and internal processes, balanced against common industry practices. Even issuing new regulatory guidance to resolve scoping ambiguities carries its own risks. Agency interpretations are inherently subject to change across administrations, particularly in an area as politically salient as online safety. This dynamic would increase the likelihood of inconsistent enforcement and undermine the stability that clear, durable legislative scoping provides.[42] Explicitly allowing covered businesses to rely on user-self-attestation avoids these problems.

23. Discuss how much the different types of age assurance methods cost and how cost is assessed.

While self-attestation frameworks can be implemented with minimal cost, age estimation and verification are substantial expenses for digital services. Third-party age verification services can cost up to $50,000 to install, plus per-user fees, costing businesses an estimated $500,000 overall.[43] Costs to implement such systems in-house are far higher, often reaching $2 million.[44]

The price of an age verification system, however, represents only part of the overall expense. Collecting sensitive data from users, proactively screening it, and properly securing it is a cost-intensive barrier to entry for smaller businesses.[45] ID requirements also deter customers and can cut businesses' conversion rates by half.[46] Furthermore, moving sensitive data across different platforms increases its vulnerability to hackers.

Startups are especially vulnerable to data breaches, as they more often need to rely on third-party vendors due to the lower up-front costs. The financial consequences of such breaches can be devastating for startups. The average cost of a data breach in 2025 was $160 per record, or $4.44 million per breach, enough to bankrupt many small companies.[47] Consequently, over 60 percent of startups close after being hacked.[48] For these reasons, the

[42] *See, e.g.*, Lieberfeld, *supra* note 20.
[43] *More Than Just a Number: How Determining User Age Impacts Startups*, Engine, 2 (last updated Aug. 2024), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/66ad1ff867b7114cc6f16b00/1722621944736/More+Than+Just+A+Number+-+Updated+August+2024.pdf.
[44] *Id.*
[45] Lieberfeld, *supra* note 20.
[46] *More Than Just a Number*, *supra* note 43, at 6.
[47] *Cost of a Data Breach Report*, IBM (2025), https://www.ibm.com/reports/data-breach.
[48] Robert Johnson III, *60 Percent Of Small Companies Close Within 6 Months Of Being Hacked*, Cybercrime (Jan. 19, 2023), https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/.

above DTSP report found that "smaller companies may not be able to sustain their business" if forced to verify user ages.[49]

24. Discuss information the AGO should consider for purposes of "commercially reasonable and technically feasible" concerning the size of a covered business for age assurance methods.

Vermont should allow businesses to implement age assurance measures that are most appropriate to the types of data they process. A business should not be required to collect data it cannot properly secure. Accordingly, regulations should align with existing standards, such as those set forth by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO). This will help businesses leverage the best existing security measures for age assurance data while avoiding duplicative compliance requirements that undermine efficiency. Such requirements should be general rather than prescriptive, requiring that businesses' security controls be reasonable and appropriate to the type, amount, and sensitivity of the information they process. This approach aligns with most existing laws and gives businesses the needed flexibility to combat security risks specific to their operations. Prescriptive requirements to institute specific security measures, by contrast, risk becoming obsolete as cyber threats evolve, imposing compliance burdens without enhancing security.

25. Discuss financial resources the AGO should consider in determining what is commercially reasonable and technically feasible for a covered business regarding age assurance methods.

While a business's financial resources are generally proportional to its ability to securely store sensitive information, there is no exact relationship between the two. As noted above, the "commercially reasonable and technically feasible" framework will inherently lead to inconsistent enforcement if self-attestation is not an option for users. The proposed rules should reflect this dynamic.

26. List and discuss technical capabilities the AGO should consider in determining what is commercially reasonable and technically feasible for a covered business regarding age assurance methods.

The AGO should consider adopting common industry frameworks for age assurance, such as those published by DTSP and ISO, as safe harbors that covered businesses can rely on to ensure compliance, as discussed below (see response to Question 30).[50] This will help ensure that covered businesses can know they are in compliance, and allows businesses to match their security practices to the type and amount of data they process. Consumer facing digital services have already built considerable consensus around mitigating content- and conduct-related risks to users and other parties. Most of the leading firms in the industry have

[49] *Age Assurance*, *supra* note 26.
[50] *See* ISO/IEC 25389:2025, *Information technology — The safe framework* (Edition 1, June 2025), https://www.iso.org/standard/90106.html; *Age Assurance*, *supra* note 26.

committed to meet best practice standards for online safety which are embedded in a recently published 2025 international standard.[51]

27. Discuss the impact using age assurance methods would have on the safety, utility, and experience of Vermonters using an online service.

Methods such as age verification that require Vermonters to share sensitive personal information substantially undermine privacy and security. Such policies run contrary to the data minimization principles underlying federal and international best practices for privacy protection.[52] Requiring individuals to share sensitive personal information with third parties, including IDs or biometrics, can make recipients a prime target for identity theft, cyberattacks, or other data breaches.[53] Such dangers are far from hypothetical: several of the most devastating data breaches in recent years are directly attributable to age verification requirements.[54]

28. Discuss what is considered an appropriate review process for an age appeal and whether the AGO should adopt certain elements, features, or steps for an appeal.

An appeals process should enable users to submit good-faith requests to change their age determination. However, allowing unlimited appeals allows malicious actors to spam covered businesses with fraudulent requests. Covered businesses would then have to divert resources away from bona fide requests in order to answer endless appeals. VDPOSA recognized this need by allowing operators the ability to ignore age appeals they believe to be fraudulent.[55] CCIA therefore recommends requiring covered operators to "provide a clear, accessible, and meaningful appeals process where appropriate, which shall be disclosed prior to the use of the service and in language that is easily understandable" rather than the proposed requirement to provide this process "for any age-related determination."[56]

29. Discuss the types of transparency measures that would help to increase consumer trust in an age assurance method.

When studying public trust of age assurance measures, a crucial pattern emerges: public support for protecting children online does not translate to willingness to upload IDs or face scans, or trust in common age assurance methods.[57] Utah State University's recent national

---

[51] *Id.*
[52] *See, e.g.*, *Fair Information Practice Principles (FIPPs)*, Fed. Privacy Council, https://www.fpc.gov/resources/fipps/; *Principle (c): Data Minimisation,* U.K. Info. Comm'r Off., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/.
[53] Shoshana Weissmann, *Age-Verification Legislation Discourages Data Minimization, Even When Legislators Don't Intend That*, R St. Inst. (May 24, 2023), https://www.rstreet.org/commentary/age-verification-legislation-discourages-data-minimization-even-when-legislators-dont-intend-that/.
[54] Mark Tsagas, *Online Age Checking Is Creating a Treasure Trove of Data for Hackers*, The Conversation (Nov. 11, 2025), https://theconversation.com/online-age-checking-is-creating-a-treasure-trove-of-data-for-hackers-268586.
[55] 9 V.S.A. § 2415d(c)(4)(C) (2026).
[56] "Age Assurance Privacy," *supra* note 2, at 10.
[57] Wagener, *supra* note 39.

survey showed two-thirds of Americans are not comfortable sharing a government ID with social media companies to verify their age, and nearly 70% are not comfortable sharing their child's ID.[58] A Carnegie Mellon University study showed that 52% were willing to undergo AI-based facial analysis, just 22-28% of participants were willing to upload their IDs for an age check, and just 17% were willing to accept a brief recording to prove they were human.[59] Similar findings have been demonstrated abroad: In the wake of the UK Online Safety Act rollout, Ipsos found public support for age checks in principle, but far less willingness to participate in common age assurance methods: only 19% would provide proof of age on dating apps, 37% for social media, and 38% for messaging services.[60] Such mandates would force Vermonters to choose between providing government IDs and face scans and accepting the associated data security risks, or losing access to online services that are critical for information, communication, and free expression.

30. Discuss whether a certification model like the Secretary of State's data broker registry would be sufficient for covered businesses to assert they comply with AADC rules.

A certification model that covered businesses can use as a safe harbor is an excellent way to ensure high standards and legal consistency. Safe harbor provisions are important for fair and effective enforcement. Safe harbors (1) provide valuable predictability to both market actors and consumers, (2) enable speedier compliance, and (3) deter vexatious, meritless litigation if in fact parties other than the state are authorized to enforce the statute. When the AGO alleges noncompliance with a privacy or security obligation, businesses should therefore be allowed to use compliance with an established privacy framework like NIST and ISO as an affirmative defense against such allegations. Businesses should also receive advance notice of complaints and have the opportunity to cure violations before enforcement actions are brought, both to minimize costly enforcement actions and focus agency resources on large-scale and repeat offenders.

31. Discuss the methods that should be considered to ensure that the privacy of user data is preserved in any age assurance method.

Many provisions of the proposed rules undermine user privacy and should be removed. Aside from the constructive knowledge standard discussed above, the proposed rules require covered businesses to "not send any push notification to a covered minor between the hours of 12:00 a.m. and 6:00 a.m.," except for transactional, safety, or account-related purposes.[61] Such requirements inevitably require that covered operators track when it is nighttime in a

[58] Taylor Barkley, *Poll: Americans Don't Want to Share Their Photo ID to Tweet*, Utah St. U. (Feb. 1, 2023), https://www.thecgo.org/benchmark/poll-americans-dont-want-to-share-their-photo-id-to-tweet/.
[59] Yanzi Lin et al., *User (Non-)Compliance with Age Verification: Preliminary Evidence from a Deceptive Web Experiment*, Carnegie Mellon U. CyLab Sec. & Priv. Inst., https://www.cs.cmu.edu/~sscheffl/docs/2026/AgeVerif2026.pdf.
[60] Keiran Pedley, *Britons Back Online Safety Act's Age Checks, but Are Sceptical of Effectiveness and Unwilling to Share ID*, Ipsos (Aug. 17, 2025), https://www.ipsos.com/en-uk/britons-back-online-safety-acts-age-checks-are-sceptical-effectiveness-and-unwilling-share-id.
[61] "Prohibited Data and Design Practices," *supra* note 1, at 11.

device's location. This requirement therefore effectively mandates location-based tracking of minors' devices, thus undermining the privacy of the very population the bill is designed to protect. Requiring covered operators to track their users serves no benefit, particularly since covered operators regularly give users the option to turn off notifications themselves.

32. Discuss whether certain data minimization practices should be adopted for AADC rules and if so, what data minimization procedures could be deployed to ensure compliance with the AADC.

Data minimization is a critical component of data security. Businesses should not be forced to collect data that they do not have the resources to process and store securely. This principle forms the foundation of longstanding privacy guidelines from the Federal Privacy Council, UK Information Commissioner, and other leading privacy authorities.[62] However, as noted above, the AGO's creation of a new knowledge standard undercuts this principle, as it incentivizes covered businesses to collect more data than they otherwise would to minimize legal exposure. The proposed rules would make privacy-invasive practices such as age verification the surest way to demonstrate compliance.

33. Discuss whether covered businesses and processors should use previously collected data to determine user age and if so, the type of data that would be most advantageous.

Businesses should be permitted to use previously collected data as an age signal where appropriate. COPPA enforcement should provide guidance regarding what types of information may be used for such purposes.[63] For instance, the length of time a user has held an account can indicate a user's minimum age, as can information in a user's bio or answers to survey questions posed by the online service, such as what grade a user is in. The AGO should adopt COPPA's guidance on which pieces of data constitute knowledge of a user's age.

34. Discuss the types of age assurance methods that are interoperable and whether the AGO should consider certain types over others and why.

Mandatory interoperability interfaces should be avoided, as they undercut user privacy. In particular, widespread consumer privacy rights like data deletion become nearly impossible to implement under such conditions: once a third party possesses a user's data, ensuring its deletion is generally infeasible.

Moreover, a public-facing interface designed for the purpose of extracting user data significantly increases the risk of data breaches. A hacker or foreign adversary accessing such an interface could obtain data from many social media users across several sites. In other key industries such as healthcare, interoperability of records has significantly increased vulnerability to cyberattacks in recent years.[64]

---

[62] *See, e.g.*, *Fair Information Practice Principles (FIPPs)*, *supra* note 52; *Principle (c): Data Minimisation, supra* note 52.
[63] *See* Lieberfeld, *supra* note 20.
[64] *See, e.g.*, Lancer Gates, *Cyber Attacks on Interoperable Electronic Health Records: A Clear and Present Danger*, 121 Mo. Med. 6, 6-9 (2024), https://pmc.ncbi.nlm.nih.gov/articles/PMC10887471/.

Different companies have different security practices. Some encrypt data while others do not. Companies also retain different types of data for different periods of time, and are bound by different laws and regulations if they operate across multiple jurisdictions, as online services tend to do. Many also tailor their security practices to the specific types of data they process. Interoperability requirements undermine companies' ability to create the best security features for their specific data uses, which in turn undermines their users' safety.

While interoperability requirements might save consumers a modicum of time when setting up a profile on a new social media site, the potential time saved is not worth the security risks. Companies should be allowed to protect their users' information in the best way possible given the configuration of their own websites without needing to water down such practices to make user data accessible to other companies.

35. Discuss the most effective, secure, private, affordable, quick, and easy-to-use, commercially reasonable, and technically feasible methods for any form of age assurance online.

The most appropriate age assurance methods will depend on a business's financial resources and the types of data they process. Ironically, by prohibiting design practices "designed to increase the frequency, duration, or intensity of a covered minor's interaction with an online service, product, or feature," the proposed rules create more legal risks for companies that invest the most in youth online safety and consumer protection. Developing online safety features for minors requires gathering data about users' ages, which leads to increased liability. Security fixes, better user features, and even improved processes for removing spam or other malicious content could therefore create additional liabilities for businesses, and thus require them to invest in costly age assurance measures. By contrast, those who avoid such investments can escape these obligations, and with it, the broad liability that attaches. Regulations should reward investments in online safety rather than deter them by tying those investments to additional legal and compliance burdens.

36. List/discuss whether there is anything else important for the AGO to consider in adopting AADC rules.

In general, far more care must be taken to adhere to the statutory mandate. The proposed rules contain many instances where the AGO has exceeded its rulemaking authority. Besides the instances noted above, the ban on secondary data use is broader than the statute permits. VAADCA allows covered businesses to "use previously collected personal data of a covered minor" for a "purpose other than a purpose for which the personal data was collected" if "necessary to comply with any obligation under this chapter."[65] However, the proposed rules do not permit secondary data uses *even if* they are necessary to comply with other VAADCA obligations, directly contradicting the statute.[66] The phrase "necessary to comply with any obligation under this chapter" should therefore be added to subsection (a) of the "Secondary Use" section. Likewise, subsections (c) and (d) of this section should be removed, as they contain activities that are not inherently secondary uses, such as model training and

[65] 9 V.S.A. § 2449f(a)(2) (2026).
[66] "Prohibited Data and Design Practices," *supra* note 1, at 5.

recommendation improvements (these practices do not even necessarily require personal data).

Other key terms are overbroad and create compliance difficulties, often worsening users' experience in the process. For instance, the phrase "specific and contemporaneous" should be removed from the definition of "express and unambiguous request," as a user typically selects account settings assuming that they will apply until the user changes them. The phrase "specific and contemporaneous" may prevent covered businesses from carrying over minors' account settings into subsequent sessions. Similarly, the proposed rules define "monitoring" such that almost any covered businesses "monitors" its users merely by running a website. Nearly all websites collect clicks and navigation patterns. This definition should be narrowed to real-time, continuous monitoring to avoid constantly requiring businesses to signal their users.

Lastly, covered businesses will not have sufficient time to institute the necessary compliance measures. The proposed rules take effect within 60 days of the comment submission deadline. Given the multitude of new practices covered businesses might need to adopt to attain compliance, CCIA recommends allowing covered businesses at least 12 months after this deadline to attain compliance.

* * * * *

While we share concerns regarding the safety of young people online and the importance of data privacy, we encourage the AGO to resist advancing regulations that pose significant compliance, privacy, and constitutional concerns, and to revise the proposed rules to ensure conformity with VAADCA.

We appreciate your consideration of these comments and welcome opportunities to provide additional feedback on this and other technology policy matters.

Sincerely,

Jesse Lieberfeld
Policy Counsel– Privacy, Security, & Emerging Technologies
Computer & Communications Industry Association

Bambara, Anthony

Subject: Comment from Front Porch Forum re Act 63 rulemaking

From: Jason Van Driesche <jason@frontporchforum.com>
Sent: Thursday, 24 September 2026 06:54:31
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: Comment from Front Porch Forum re Act 63 rulemaking

Some people who received this message don't often get email from jason@frontporchforum.com. Learn why this is important
EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

To whom it may concern:

Attached please find Front Porch Forum's comments for the AGO regarding Act 63 rulemaking. Please reach out with any questions.

Best,
Jason

Jason Van Driesche
Chief of Staff
Front Porch Forum
jason@frontporchforum.com

front porch forum®
HELPING NEIGHBORS CONNECT

Input on the Act 63 Age-Appropriate Design Code Rulemaking

September 23, 2026

Dear Attorney General Clark and Age-Appropriate Design Code Rulemaking Team,

I am writing on behalf of Front Porch Forum (FPF) to encourage you to adopt the proposed rules for Sections 2249f and 2449g of Act 63. We are a "covered business" under Act 63, and strongly support both the goals of this law and the rules as written.

FPF already applies the design principles outlined in the law to all of our members regardless of age. We believe that all Vermonters deserve to be free from compulsive use, privacy invasion, and surveillance.

Front Porch Forum's mission is to help neighbors connect and build community. The practices commonly employed by Big Tech platforms are antithetical to this mission. Therefore, as you will see below, FPF's practices are already in keeping with the provisions of Act 63.

Data privacy

- FPF collects the least data needed in order to provide our community-building service and ensure members comply with our Terms of Use.
- We respect member privacy and do not sell member data to third parties.

Built-in safety features

- Members are required to use their real first and last name and street address to sign up for FPF, which leads to higher accountability for online actions.
- We do not have "member profiles" - so member information is not available to other members until and unless a member chooses to post to their forum.
- FPF protects members' email addresses by providing an email relay service, such that a posting author's email address is not revealed unless the member chooses to share their contact information by replying to a direct message.
- Full contents of postings are viewable only by other FPF members within a limited geographic radius (semi-anonymized content may be more broadly available).
- All content is reviewed by trained FPF moderation staff before publication, and staff members routinely scan for possible safety concerns in postings.

Designed for healthy - not compulsive - engagement

- FPF is intended to be a brief daily habit, not a harmful and time-eating addiction: our design goal is that FPF members should tune into their local Forum for 10 minutes or so each day, then engage with neighbors in real life.
- FPF displays a finite amount of content to members each day: members have to actively seek out additional content, and are not presented with a continuous scroll of endless content.
- FPF does not profile members or track member behavior, and does not use an engagement-oriented algorithm to deliver individually targeted content; instead, all members receive the same content at the same time as all others in their Forum.
- Finally, push notifications are only sent when a new Forum issue is available (approximately once per day, during daytime hours), and can be declined by members upon signing up for the mobile app or in their settings.

In summary, our business is already compliant with the spirit of the law, as well as with the vast majority of the specific provisions. Any changes we need to make to ensure full compliance are minor. Again, we encourage you to adopt the rules as written, and to support the strongest possible measures to protect Vermonters from the harms of Big Tech.

Sincerely,

Michael Wood-Lewis, Co-Founder & CEO
Front Porch Forum

Bambara, Anthony

Subject: KGI Comments on Vermont AADC Rulemaking, Sections 2449g

From: Amy Winecoff <amy.winecoff@georgetown.edu>
Sent: Friday, 25 September 2026 14:30:51
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Cc: Alissa Cooper <alissa.cooper@georgetown.edu>
Subject: KGI Comments on Vermont AADC Rulemaking, Sections 2449g

Some people who received this message don't often get email from amy.winecoff@georgetown.edu. Learn why this is important
EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Dear Office of the Vermont Attorney General,

On behalf of the Knight-Georgetown Institute (KGI), please find attached our comments on the proposed rules for Sections 2449g on implementing the age assurance provisions of Vermont's Age-Appropriate Design Code.

Our comments focus on the scope of the proposed requirements, privacy protections, evaluation and accuracy standards, documentation, transparency, and independent certification. We appreciate the opportunity to provide input on the proposed rules and the Attorney General's consideration of these implementation issues.

Please let us know if you have any questions or if we can provide any additional information.

Best regards,

--
Amy Winecoff, PhD
Senior Technologist
Knight-Georgetown Institute (KGI)
https://kgi.georgetown.edu/

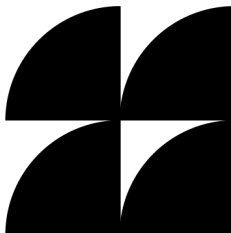
Knight Georgetown Institute

SEPTEMBER 25, 2026

Vermont Office of the Attorney General's Age-Appropriate Design Code Notice of Proposed Rulemaking

Knight-Georgetown Institute (KGI) Comments

Amy Winecoff
Alissa Cooper
Knight-Georgetown Institute





About the Knight-Georgetown Institute

The Knight-Georgetown Institute (KGI) is dedicated to connecting independent research with technology policy and design. KGI serves as a central hub for the growing network of scholarship that seeks to shape how technology is used to produce, disseminate, and access information. KGI is designed to provide practical resources that policymakers, journalists, and private and public sector leaders can use to tackle information and technology issues in real time. Georgetown University and the Knight Foundation came together to launch the institute in 2024. Learn more about KGI at https://kgi.georgetown.edu.

Table of Contents

I. Introduction....1
II. Scope....2
A. The selection of age assurance methods should not be based on proportionality.... 3
B. Age assurance should be triggered only when users seek to access prohibited services, products, or features....4
C. Guardrails must apply to both minors and adults....4
D. Recommended changes to proposed Rule text....5
III. Privacy....6
A. Zero-knowledge proofs should be required once technically feasible....7
B. The graduated escalation framework should be eliminated....7
C. Age assurance data should be retained long enough to support the appeals process.... 8
D. Age assurance data should not be used for advertising of any kind....8
E. The deletion obligation should not be limited to “raw personal data”....8
F. Self-declaration should be limited to parents....9
G. Recommended changes to proposed Rule text....9
IV. Evaluation and Accuracy Standards.... 11
A. Age assurance systems should be required to meet a quantitative accuracy standard....11
B. Required accuracy minimums and collective exclusion rates should apply to both aggregate and subgroup analyses.... 12
C. Recommended changes to proposed Rule text....13
V. Documentation.... 14
A. The documentation of evaluations should be comprehensive.... 15
B. Recommended changes to proposed Rule text.... 15
VI. Transparency & Certification.... 16
A. Covered businesses should be required to make documentation public.... 16
B. Covered businesses should obtain annual certification of their age assurance systems from an accredited third-party evaluator.... 17
C. Recommended changes to proposed Rule text....18
VII. Appendix....19
VIII. References....22

I. Introduction

The Knight-Georgetown Institute (KGI) is dedicated to connecting independent research with technology policy and design. Based at Georgetown University in Washington, D.C., KGI serves as a hub for the growing network of scholarship that seeks to shape how technology is used to produce, disseminate, and access information. KGI is designed to provide practical resources that policymakers, journalists, and private and public sector leaders can use to tackle information and technology issues in real time.

KGI welcomes the opportunity to inform the Vermont Age-Appropriate Design Code (AADC) Rulemaking and appreciates the Attorney General's engagement with independent research and implementation considerations in this process.

We appreciate many aspects of the proposed Rule. In particular, the proposed Rule requires covered businesses to provide fallback mechanisms that minimize additional data collection and avoid unnecessary reliance on methods with large privacy risks; establishes a meaningful appeals process; includes sensible restrictions on the collection, retention, secondary use, and disclosure of age assurance data; limits repeated or continuous reassessment and monitoring; requires businesses to consider accessibility and disparate burdens on certain user groups; and makes covered businesses responsible for the conduct of third-party age assurance providers. These provisions reflect thoughtful attention to the privacy, accessibility, and implementation risks that age assurance can create.

At the same time, aspects of the proposed Rule could be further clarified or strengthened to ensure that covered businesses implement effective age assurance systems with adequate safeguards. The proposed Rule could be further strengthened through the revisions described in our comment, which draw on KGI's technical evaluation of existing age assurance systems[1] and analysis of how those findings can inform implementation.[2] KGI's prior work in these areas has focused on how age assurance systems can help reduce minors' exposure to potentially harmful online experiences while avoiding unnecessary risks to the privacy, autonomy, access to information, and freedom of expression of all users.

KGI recommends several revisions to strengthen the proposed Rule. These include eliminating the proportionality and graduated escalation provisions to establish clearer and more uniform requirements for age assurance implementation and extending relevant safeguards to all users subject to age assurance, not just covered minors. The Rule should also establish quantitative accuracy standards and require more comprehensive evaluation and documentation of system performance,

[1] Eric Rescorla et al., *Age Assurance Online: A Technical Assessment of Current Systems and Their Limitations* (Knight-Georgetown Institute, 2026), https://kgi.georgetown.edu/research-and-commentary/age-assurance-online/.
[2] Amy Winecoff and Alissa Cooper, *Age Assurance Rules: An Implementation Guide* (2026), https://kgi.georgetown.edu/research-and-commentary/age-assurance-rules-implementation/.

including evaluation methods, system configurations, testing data, limitations, and mitigation measures. Greater transparency and accountability mechanisms should accompany these requirements through public reporting of age assurance assessments and annual independent evaluation and certification.

Our comments are organized as follows:

- Section II addresses the scope of the proposed Rule, including proportionality and the application of age assurance safeguards to both minors and adults;
- Section III discusses privacy protections, including zero-knowledge proofs, graduated escalation, data retention and deletion, advertising uses, and parental declaration;
- Section IV addresses evaluation and accuracy standards, including quantitative performance requirements and subgroup evaluation;
- Section V discusses documentation requirements; and
- Section VI focuses on transparency, independent evaluation, and certification.

II. Scope

The proposed Rule defines the scope of its age assurance requirements in three important ways. First, it adopts a proportionate framework under which covered businesses determine how age assurance requirements apply based on the risks of a particular service, product, or feature and the characteristics of the age assurance method used. Second, the proposed Rule would require all covered businesses to implement age assurance, regardless of whether the business offers an online service, product, or feature that is prohibited for minors within the proposed Rule 2449f, or whether a user is seeking to access such a service, product, or feature. Third, although age assurance necessarily involves determining the age of users who may ultimately be either minors or adults, many of the Rule's safeguards governing the age assurance process are framed specifically as protections for "covered minors."

We recommend revising all three aspects of the proposed Rule's scope. Rather than relying on largely unspecified proportionality assessments, the Rule should apply a common set of age assurance requirements to the subset of covered businesses already subject to obligations under the AADC when they offer online services, products, or features that fall within the prohibitions of proposed Rule 2449f. Because the goal of age assurance broadly is to protect youth from risky online experiences rather than gate online experiences regardless of risk, the obligation to conduct age assurance should arise only when a user seeks to access a service, product, or feature prohibited for minors. In addition, safeguards governing the age assurance process itself, such as protections related to privacy, accessibility, user burden, fallback mechanisms, and appeals, should generally apply to all users undergoing age assurance, regardless of the age determination ultimately reached.

A. The selection of age assurance methods should not be based on proportionality

The proposed Rule adopts a flexible, proportionate framework, which gives covered businesses substantial discretion to determine whether and how they implement age assurance. The proposed Rule approaches this by defining "proportionate age assurance" as "an age assurance process or technique calibrated to the risks posed by an online service, product, or feature and implemented using the least intrusive means reasonably available" (Definitions section (k)). This definition, and the notion of proportionality, is embedded throughout the proposed Rule.

Under this framework, businesses would make qualitative judgments about system specifications, such as the level of accuracy required and acceptable degree of intrusiveness, without specific criteria in the proposed Rule to guide those decisions. This approach leaves covered businesses placing risky products and features into the market with considerable latitude to select age assurance methods that are widely understood to be ineffective. This construction also creates ambiguity for businesses about whether their implementation choices satisfy the proposed Rule's requirements. The proposed Rule likewise provides no clear accountability mechanism for assessing whether those judgments are reasonable.

We recommend instead applying the same age assurance standards to all covered businesses with obligations under 9 V.S.A. § 2449c (minimum duty of care), § 2449d (default privacy settings), or § 2449f(a)(3-5) (prohibited design practices). In other words, rather than applying an ambiguous notion of proportional age assurance to all covered businesses based on their own subjective judgment of risks, apply the same (non-proportional) age assurance requirements to the subset of covered businesses offering products, services, or features that the law already recognizes as risky: those that can lead to covered minors' reasonably foreseeable emotional distress, compulsive use, or discrimination; those that offer features subject to default privacy settings; or those that support location tracking, recommender systems, or push notifications. Imposing a uniform framework would ensure that all covered businesses offering such features are held to the same standards and would reduce ambiguity about which requirements apply based on a largely unspecified risk assessment.

We recommend removing all aspects of the proposed Rule linked to proportionality. Although eliminating this framework could potentially encourage covered businesses to adopt a more intrusive approach, the Rule's existing privacy protections along with the additional modifications we recommend below can mitigate this risk. In place of proportionality, we recommend that the proposed Rule specify that whenever a covered business is required to conduct age assurance, the age assurance system it implements, as well as the governance processes used to manage and oversee that system, must satisfy all applicable requirements of the Rule.

B. Age assurance should be triggered only when users seek to access prohibited services, products, or features

The proposed Rule 2449f, which establishes requirements related to prohibited data and design practices, prohibits both: 1) any service, product, or feature determined to create a reasonably foreseeable heightened risk of harm to covered minors; and 2) specific design practices that Rule 2449f independently prohibits or restricts as applied to covered minors, regardless of whether a separate heightened-risk determination is made. The proposed Rule 2449g, however, would require all covered businesses to conduct age assurance regardless of whether that business offers an experience that falls into either category or whether users are seeking to access those experiences.

Requiring covered businesses to conduct age assurance even when no such prohibited or heightened-risk experience is available — or before a user seeks to access one — would impose privacy, access, and usability burdens on users without advancing the Rule's protective purpose. Because age assurance itself carries costs and risks, those burdens are justified only when necessary to determine whether a user may access a service, product, or feature from which covered minors must be protected.

We recommend that the proposed Rule explicitly provide that a covered business's obligation to conduct age assurance is triggered only when the business offers an experience prohibited for covered minors under proposed Rule 2449f and a user seeks to access that experience.

C. Guardrails must apply to both minors and adults

Vermont's AADC is intended to protect minors from harms associated with the risky products, services, and features of covered businesses. Age assurance is therefore an important component of implementing the AADC because to provide protections to minors, covered businesses must first have some means of determining which users are minors. But age assurance systems do not affect minors alone. Adults who are required to undergo age assurance may face the same usability burdens and risks to privacy, security, and access to information that these systems pose to minors.

Throughout the proposed Rule, however, important safeguards governing age assurance are framed as protections specifically for "covered minors." This creates ambiguity about whether covered businesses must provide comparable protections to adult users who are also subject to age assurance. Given both the risks associated with age assurance and the potential sensitivity of the data collected, processed, or transmitted through these systems, limiting these safeguards to minors could leave adult users exposed to significant risks.

As one example, several restrictions on data use are expressly tied to covered minors. As drafted, a covered business could reasonably interpret these provisions to mean that, once a user is determined to be an adult, it is no longer required to minimize the linkability of that user's age-assurance data or to limit retention and use in ways that prevent tracking, profiling, advertising, or cross-service identification. The proposed Rule should instead make clear that safeguards governing the collection,

processing, retention, disclosure, and use of age-assurance data apply to all users subjected to age assurance, regardless of the age determination ultimately reached.

The proposed Rule implementing Section 2449f separately establishes the requirements that covered businesses must apply specifically to minors. By contrast, age assurance under Section 2449g is the process businesses use to determine which users are minors and therefore must be applied to users of any age.

We recommend that safeguards governing the age assurance process should accordingly apply to all users subjected to it.

D. Recommended changes to proposed Rule text

We suggest the changes below to effectuate the recommendations made throughout Section II.

In the Applicability section, update:

> (a) This Rule regulates the collection, use, and processing of data in age assurance systems and is intended to govern business conduct and system design. The Rule does not mandate the use of any specific technology, does not require identity-based age verification, and does not restrict access to particular content. ~~It adopts a flexible, proportionate framework to protect covered minors and minimize privacy concerns.~~ Nothing in this Rule shall be construed to require monitoring of a covered minor's activity beyond what is reasonably necessary to implement age assurance.
> (b) This Rule applies where: ~~a covered business knows or reasonably should know that a user is a covered minor.~~
>
> **i. A covered business offers an online service, product, or feature prohibited under Rule 2449f; and**
>
> **ii. A user seeks to access such an experience.**
>
> ~~(c) A covered business shall implement proportionate age assurance measures for any online service, product, or feature reasonably likely to be accessed by covered minors.~~
> (d) A covered business shall determine whether a user is a covered minor using ~~a proportionate~~ **an age assurance method that satisfies each of the system requirements set forth in this Rule.**
> **(e) A covered business shall establish and maintain governance processes for the implementation and oversight of that method in accordance with the applicable requirements of this Rule.**
> ~~(e) Age assurance shall be conducted using the least intrusive age assurance process or technique reasonably available that achieves the reasonably necessary level of confidence.~~

In the Definitions section, delete:

> ~~(k) "Proportionate age assurance" means an age assurance process or technique calibrated to the risks posed by an online service, product, or feature and implemented using the least intrusive means reasonably available.~~
>
> ~~1. An age assurance process or technique is not proportionate where a less intrusive age assurance process or technique would reasonably achieve a comparable level of accuracy.~~
> ~~2. Proportionate age assurance shall be evaluated based on:~~
> ~~i. Privacy impact and data minimization;~~
> ~~ii. Accessibility and ease of use for covered minors;~~
> ~~iii. The burden imposed on covered minors;~~
> ~~iv. The sensitivity and risk profile of the online service, product, or feature;~~
> ~~v. The availability of less intrusive alternatives; and~~
> ~~vi. The reasonably necessary level of accuracy or confidence required for age determination.~~

Throughout the rule, delete references to proportionality and delete the Age Assurance Selection section.

For each provision listed within the Appendix of our comment, replace "covered minor" with "consumer" as defined in the AADC.

III. Privacy

The proposed Rule includes extensive privacy protections governing the collection, use, retention, disclosure, and combination of data used for age assurance. It also seeks to reduce privacy risks through data minimization, limits on linkability and secondary uses, restrictions on persistent monitoring and repeated reassessment, and requirements that businesses use less intrusive approaches where reasonably available. These provisions provide a strong foundation of privacy protection for consumers undergoing age assurance.

Several targeted changes could build upon that foundation. We recommend that the Rule eliminate the graduated escalation framework; require the use of methods employing zero-knowledge proofs once they are technically feasible; and strengthen deletion and retention requirements so that they cover derived and combined data created solely for age assurance. We also recommend additional requirements for data use for advertising and appeals and modifications for self-declaration as a method of age assurance.

A. Zero-knowledge proofs should be required once technically feasible

The proposed Rule requires covered businesses to limit the collection, disclosure, retention and use of age assurance data. These requirements are important safeguards, but do not provide consumers with verifiable guarantees that the covered business has implemented data protections correctly.

Zero-knowledge proofs (ZKP) allow consumers to demonstrate their eligibility while revealing no other information about themselves to covered businesses or other third parties such as age verification providers. Because these techniques have technical privacy guarantees, they do not require the user to trust the covered business.

We therefore recommend that the proposed Rule include a definition for ZKPs to the Definitions section and a requirement for covered businesses to use a ZKP-based age assurance method once technically feasible, specifically when one or more of the mobile operating system vendors with the highest market penetration in Vermont offer a ZKP-based age assurance method implementing a publicly available ZKP technical specification and age assurance protocol.[3]

B. The graduated escalation framework should be eliminated

The proposed Rule categorizes the intrusiveness of age assurance processes or techniques largely according to the types of signals on which they rely: self-declaration, existing age signals, and certain contextual indicators are associated with low-intrusion approaches; device, account, and usage data with moderate-intrusion approaches; and credentials or documentation with higher-intrusion approaches.

While we applaud Vermont's effort to encourage the use of the least privacy-invasive age assurance techniques possible, the proposed Rule does not operationalize intrusiveness in a way that reflects how age assurance systems actually work. A system's intrusiveness depends not only on the type of age signal it uses, but also on a range of implementation choices, including where processing occurs, what information is transmitted or retained, and whether the resulting age-related determination can be linked across services or contexts.

For example, an age assurance system could rely on a digital identity credential stored on the consumer's device while using a zero-knowledge proof or similar privacy-preserving protocol to reveal only the consumer's age range to the covered business. Although the proposed Rule would classify credential-based age assurance as higher intrusion, this particular implementation could disclose very little information and impose substantially less privacy risk than other systems relying on ostensibly less intrusive signals as defined by the proposed Rule.

[3] We note that requirements for implementing a ZKP-based age assurance method would apply only in mobile environments. However, because minors are most likely to access covered businesses' services through mobile devices, this is also the context in which both age assurance and the safeguards governing its use are most important.

More generally, the privacy implications of an age assurance system cannot be inferred from the underlying age signal alone. A potentially sensitive signal can be used within a highly privacy-preserving architecture, while a less sensitive signal can be implemented in ways that involve broader collection, transmission, retention, or linkability. For this reason, system designs cannot be coherently ranked by intrusiveness based primarily on the type of age assurance method or signal they employ.

The proposed Rule already includes robust provisions for privacy protection and data management. The graduated escalation framework within the proposed Rule does little to ensure privacy above those existing privacy requirements. By adding provisions requiring zero-knowledge proofs as we recommend, the Rule will also require additional technical privacy guarantees when they become technically feasible to implement.

We recommend removing all requirements related to graduated escalation.

C. Age assurance data should be retained long enough to support the appeals process

The Data Minimization in Age Assurance section identifies limited circumstances in which age assurance data may be retained beyond completion of the age assurance process. The Rule should also allow for retention for the limited period necessary to support an appeal where data used in the initial age determination may be relevant to resolving that appeal. Once the period for filing an appeal has expired or, if an appeal is filed, once it has been resolved, those data should be deleted unless another permitted basis for retention applies.

D. Age assurance data should not be used for advertising of any kind

Linkability and System Design subsection (b)(4) prohibits use of age assurance data for "behavioral advertising." The word "behavioral" should be deleted. Age assurance data should not be used for contextual, demographic, age-targeted, or any other advertising purpose. This change would also make the provision consistent with other parts of the draft that more broadly prohibit use of age assurance data for secondary purposes.

E. The deletion obligation should not be limited to "raw personal data"

Data Minimization subsection (d) requires deletion of "raw personal data used for age assurance." That formulation is too narrow. Age assurance may create derived variables, intermediate outputs, combined datasets, or other information that creates privacy or linkability risk even where it is no longer "raw" or is not obviously identifying in isolation.

The deletion obligation should therefore cover any additional data collected solely for age assurance; derived or intermediate data generated solely for age assurance; and datasets created by combining new or existing information for the sole purpose of age assurance.

We recommend these data be deleted once they are no longer necessary to complete age assurance, taking into account a period of time that allows for recourse, or as required for auditing or evaluation.

F. Self-declaration should be limited to parents

Within the existing Graduated Escalation categories, the Rule lists "self-declaration mechanisms used in combination with reasonable safeguards" as a form of low-intrusion age assurance. Where users have an incentive to misrepresent their age, self-declaration offers little protection against circumvention and therefore cannot provide meaningful confidence that age-based requirements are being applied to the correct users.

Instead of treating self-declaration by a covered minor as a low-intrusion age assurance method, the Rule should permit a parent or guardian to declare a covered minor's age status where the parental relationship has already been established through a mechanism that does not require additional, intrusive verification of the parent. That relationship could be established through a device- or operating-system-level family configuration or through a parent or guardian account persistently linked to the minor's account.

We recommend including parental declaration as one of the possible age signals listed in Data Minimization in Age Assurance, section (c).

G. Recommended changes to proposed Rule text

We suggest the changes below to effectuate the recommendations made throughout Section III.

In the Definitions section, add:

> **(m) "Zero-knowledge proof age assurance" means a cryptographic technique that allows an individual to demonstrate age status using verified data without revealing additional information to the operator or any third-party beyond the validity of the individual's age status.**
>
> **"Parental declaration" means a parent or guardian providing a covered minor's age or age range on the minor's behalf where the parent-child or guardian-child relationship has already been established through a persistent account, device, or operating-system configuration that does not require additional verification of the parent's identity, age, or relationship to the minor.**

In the Definitions section, delete:

> ~~(i) "Highly intrusive age assurance" means an age assurance process or technique that involves the collection or processing of biometric data, identity documentation, persistent identifiers,~~

~~sensitive personal data, or other data practices that create a significant risk of linkability to a covered minor.~~

Delete the Graduated Escalation section.

In the Data Minimization in Age Assurance section, add:

(a) A covered business shall limit the collection, processing, retention, and use of personal data to what is strictly necessary to determine whether a user is a covered minor, **inclusive of the appeals process.**

(c) [...] a covered business shall use:

[...]

5. Parental declaration

(f) Where a covered business adopts a credential-based age assurance method, the covered businesses shall adopt a zero-knowledge proof age assurance method once technically feasible, specifically once one or more of the two mobile operating system vendors with the highest market penetration in Vermont provides a zero-knowledge proof age assurance method that implements a publicly available zero-knowledge proof technical specification and age assurance protocol.

In the Data Minimization in Age Assurance section, delete:

(b) A covered business shall not:

[...]

3. Retain ~~raw~~ personal data used for age assurance beyond the point of determination;

(c) [...] a covered business shall use:

[...]

4. Local or device-level processing that does not require transmission of ~~raw~~ personal data;

(d) A covered business shall delete ~~raw~~ personal data used for age assurance immediately after the age-related determination is made, except where retention is strictly necessary for: [...]

In the Linkability and System Design section, delete:

(e) A covered business shall not retain or use age assurance data in a manner that enables tracking, profiling, ~~behavioral~~ advertising [...]

IV. Evaluation and Accuracy Standards

The proposed Rule requires covered businesses to evaluate the accuracy of their age assurance systems, including false positives and false negatives, but it does not establish clear quantitative performance requirements or fully account for users who are unable to obtain an age-related determination. We recommend strengthening these provisions by defining distinct measures for false acceptances, false rejections, and system-level exclusion; establishing quantitative performance thresholds for each relevant measure; and removing the undefined concept of "confidence." We also recommend applying these accuracy requirements to both aggregate and subgroup evaluations.

A. Age assurance systems should be required to meet a quantitative accuracy standard.

The proposed Rule relies repeatedly on the "reasonably necessary level of accuracy or confidence," but does not define either "accuracy" or "confidence" or establish concrete criteria for determining what level is sufficient. Although the proposed Rule defines "error rate" and requires covered businesses to evaluate false positives and false negatives,[4] it ultimately leaves the required level of performance to a qualitative judgment, including by prohibiting only methods whose error rates create a "material risk" of misclassifying covered minors.

Accuracy is particularly well suited to a more concrete standard because it can be measured directly both before and after deployment. A covered business's age assurance system should be evaluated against two distinct accuracy goals:

- Correctly identifying consumers who meet the definition of "covered minors" so that they receive the protections required for covered minors (minimize the false acceptance rate).
- Correctly identifying consumers who are not covered minors so that they are not incorrectly subjected to those protections (minimize the false rejection rate).

These two error rates should be evaluated and reported separately because improvements in one can come at the expense of the other. While the proposed Rule recognizes both types of error, it does not clearly require separate performance standards for each or establish quantitative thresholds governing either one.

A further challenge is that returning an age-related determination is not the same as returning a correct age-related determination, which is particularly relevant for methods of age assurance that return responses with some level of uncertainty. A facial age estimation system may be able to generate an

[4] The proposed rule uses "false negative" to refer to minors classified as adults; however, we recommend using the term "false acceptance" in our comments and recommend that the proposed Rule replace "false negative" and "false positive" with "false acceptance" and "false rejection" for clarity.

estimate for nearly every user who provides a sufficiently high-quality image while still incorrectly classifying some adults as minors or some minors as adults.

More broadly, a successful age assurance outcome is one in which the system reaches the correct age-related determination. Failures, therefore, include both incorrect classifications and cases in which a user is unable to establish their age through any of the methods made available. Determining the full rate of failure therefore requires evaluating the age assurance system as a whole, because testing individual methods alone cannot establish how many users ultimately remain unable to demonstrate their age.

We recommend replacing the definitions for "false positive" and "false negative" (which are ambiguous and can be confusing) with "false acceptance" and "false rejection;" and revising the definition of "error rate" to reflect that terminology. We also recommend including a definition and requirement for "collective exclusion rate" to capture both instances in which the system falsely rejects a user and instances in which the system is unable to make any determination. In addition, the proposed Rule should provide a quantitative threshold that companies' age assurance systems are required to meet. Every instance within the proposed Rule that provides a stipulation based on "accuracy" or "confidence" should be updated to stipulate that the system must meet the accuracy minimum and the collective maximum exclusion rate.

We note that many age assurance methods are likely to have higher error rates for users closer to the age threshold. For example, a facial age estimation system will generally have greater difficulty distinguishing a 17-year-old from an 18-year-old than distinguishing a 17-year-old from a 42-year-old. The proposed Rule could therefore be further strengthened by establishing different accuracy minimums for different age bands. The New York Attorney General's rules implementing the SAFE for Kids Act provide one example of this type of graduated accuracy standard.[5]

Throughout the proposed Rule, the text references the undefined concept of "confidence." In statistics, "confidence" often refers to the degree of certainty associated with an estimate. Since the proposed Rule does not provide a definition for "confidence," we also recommend deleting every instance of this term.

B. Required accuracy minimums and collective exclusion rates should apply to both aggregate and subgroup analyses.

The draft appropriately requires covered businesses to assess whether error rates disproportionately affect particular groups, but it does not specify which characteristics must be evaluated or establish performance requirements for relevant subgroups.

Age is one important source of variation in system performance, but performance may also vary across other user characteristics. Some age assurance techniques, including facial age analysis, have

[5] New York Attorney General, "SAFE for Kids Act Implementing Rules," July 28, 2026, https://ag.ny.gov/safe-for-kids-act-final-rule.

demonstrated differences in performance across demographic groups, including individuals with different skin tones.[6] As a result, a system may satisfy an aggregate accuracy standard while performing substantially worse for particular groups of users.

The Accuracy and Error Evaluation section requires covered businesses to evaluate whether errors disproportionately affect certain groups, but it does not require deployed systems to meet minimum performance standards within those groups. At minimum, subgroup evaluations should include race, gender, and disability status. Covered businesses should also evaluate additional characteristics where they are relevant to the particular method or deployment, including language, geographic region, or other factors reasonably likely to affect system performance.

This requirement need not require covered businesses to collect these characteristics from users in production. Businesses could instead rely on appropriately designed evaluation datasets that reflect the characteristics of their user populations.

Once the Rule establishes quantitative accuracy and collective exclusion thresholds overall, those same or comparable standards should also apply to relevant subgroup analyses. We therefore recommend that the proposed Rule require deployed age assurance systems to meet the applicable quantitative accuracy minimums and collective exclusion rate both in aggregate and within specified relevant subgroups.

C. Recommended changes to proposed Rule text

We suggest the changes below to effectuate the recommendations made throughout Section IV.

In the Definitions section, add:

> **"Accuracy minimum" means a false acceptance rate for an age assurance process or technique equal to or less than [X_1% of minors ages 0 to 7; X_2% of minors ages 8 to 13; X_3% of minors ages 14 to 15; X_4% of minors age 16; X_5% of minors age 17], excluding failures by the system to make an age-related determination or refusals by a user to provide requested information. The applicable accuracy minimum must be satisfied both in the aggregate and within each subgroup required to be evaluated under the Rule, including subgroups defined by race, gender, and disability status, as well as any additional characteristics reasonably likely to affect the performance of the age assurance process or technique.**
>
> **"Collective exclusion rate" means the overall percentage of consumers who either receive a false rejection or are unable to obtain an age-related determination through any of the methods offered by the covered business.**

[6] Patrick J. Grother et al., *Face Analysis Technology Evaluation: Age Estimation and Verification*, NIST IR 8525 (National Institute of Standards and Technology (U.S.), 2024), NIST IR 8525, https://doi.org/10.6028/NIST.IR.8525.

> "Collective maximum exclusion rate" means a collective exclusion rate for all of the age assurance methods offered by the covered business that is equal to or less than [Y%]. **The applicable collective maximum exclusion rate must be satisfied both in the aggregate and within each subgroup required to be evaluated under the Rule, including subgroups defined by race, gender, and disability status, as well as any additional characteristics reasonably likely to affect the performance of the age assurance process or technique.**
>
> **"False acceptance" means a minor has been incorrectly classified as an adult.**
>
> **"False rejection" means an adult has been incorrectly classified as a minor.**

In the Definitions section, update:

> (g) "Error rate" means the ~~frequency of incorrect determinations, including false positives (adult classified as minor) and false negatives (minor classified as adult).~~ **percentage of consumers receiving incorrect determinations, including false acceptances and false rejections.**

In the Accuracy and Evaluation section, update:

> (b) Evaluation shall include:
> 1. False ~~positives~~ **rejections**;
> 2. False ~~negatives~~ **acceptances**;
> 3. **Collective exclusion rate**;
>
> [...]
>
> (d) A covered business shall evaluate whether error rates, **including with respect to race, gender, and disability status at a minimum:** [...]

Throughout the proposed Rule, replace:

> Every instance of "accuracy" or "confidence" with a stipulation that covered businesses must meet the accuracy minimum and collective maximum exclusion rate.

V. Documentation

Documentation can serve multiple governance functions for technology systems. Internally, it can inform stakeholders about system uses and risks, facilitate communication and collaboration, support more robust deliberation about potential harms, and encourage best practices in software

development and risk management.[7] Documentation produced for external stakeholders can serve many of these same functions while also supporting accountability. The proposed Rule requires covered businesses to maintain documentation sufficient to demonstrate compliance, and the Compliance and Oversight section specifies documentation requirements for age assurance assessments, including method selection, accuracy evaluations, and assessments of disparate impacts. These requirements could be strengthened by specifying additional information that covered businesses must document and by requiring that relevant documentation be made publicly available.

A. The documentation of evaluations should be comprehensive.

Evaluation methods. The Accuracy and Error Evaluation subsection (b) requires covered businesses to disclose their methodologies, sampling approaches, assumptions, and testing conditions. Each is an important component of adequate system documentation. However, the proposed Rule should also require covered businesses to document the system configurations used during testing and to evaluate all configurations they are reasonably likely to deploy. Covered businesses should also document the characteristics of the test data in detail or provide a representative sample of that data. More generally, the documentation should be sufficiently detailed to allow an accredited third-party evaluator (See Section VI. Transparency & Certification), using comparable methods and conditions, to reproduce the covered business's results within a reasonable margin of error.

B. Recommended changes to proposed Rule text

We suggest the changes below to effectuate the recommendations made throughout Section V.

In the Compliance and Oversight section, update to:

(b) Scope of Assessment. The assessment shall include:

1. Selection~~, escalation,~~ and implementation decisions relating to age assurance processes or techniques, **including the circumstances in which each age assurance method is applied, the basis for fallback decisions, and any additional implementation decisions likely to affect the performance or risks posed by the system;**
2. Accuracy and error evaluation results, including ~~false positives, false negatives~~ **false acceptances, false rejections, overall rejection rate,** known limitations, **and subgroup analyses;**
3. **The methodologies, sampling approaches, assumptions, testing conditions, and system configurations used to evaluate accuracy and other aspects of system performance, including evaluation of all configurations the covered business uses or is reasonably likely to deploy;**

[7] Amy Winecoff and Miranda Bogen, "Improving Governance Outcomes Through AI Documentation: Bridging Theory and Practice," *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, April 26, 2025, 1–18, https://doi.org/10.1145/3706598.3713814.

4. **The characteristics of the data used for evaluation, in sufficient detail to assess its relevance and representativeness, or — where doing so would not create material privacy or security risks — a representative sample of the evaluation data;** [...]

(d) Documentation Requirements. A covered business shall maintain documentation reasonably sufficient to demonstrate compliance with this Rule, including documentation of each assessment required under subsection (b).

VI. Transparency & Certification

The proposed Rule requires covered businesses to conduct a comprehensive assessment of their age assurance systems and maintain documentation sufficient to demonstrate compliance. However, it relies largely on covered businesses to assess and document their own systems, without requiring either public disclosure of those assessments or independent review of their adequacy. We recommend strengthening these accountability mechanisms in two ways: 1) by requiring covered businesses to provide the Office of the Attorney General with their documentation and make an accessible version of the documentation publicly available; and 2) by requiring at least annual evaluation and certification by an accredited third-party evaluator.

A. Covered businesses should be required to make documentation public.

The proposed Rule does not require covered businesses to provide that documentation to the Office of the Attorney General, any independent third parties, or the public. Without the ability for any authority or outside expert to review any version of these assessments (even in redacted form), their utility as an accountability mechanism will be severely limited.

Covered businesses should be required to provide a public, accessible, and up-to-date version of their documentation, subject to narrowly-tailored protections where detailed disclosure would materially facilitate circumvention or otherwise risk revealing sensitive information. Detailed public documentation would enable stakeholders outside the formal compliance ecosystem to scrutinize the choices covered businesses make in designing and deploying age assurance systems. It would also enable researchers to conduct evaluations that more closely reflect real-world deployments and to assess the plausible individual and societal impacts of those systems. Such evaluations have already proved valuable in assessing how realistic age assurance systems function in practice.[8] Public documentation could also help researchers, technologists, and civil society identify potential weaknesses or vulnerabilities that the covered businesses' own assessments failed to address and communicate them to covered businesses so that they can be mitigated.

[8] Shreyas Minocha et al., "Papers, Please: A First Look at Age Verification on the Web," *2026 IEEE Symposium on Security and Privacy (SP)*, May 2026, 4185–202, https://doi.org/10.1109/SP63933.2026.00161; Olivia Figueira et al., "Actions Speak Louder Than Chats: Investigating AI Chatbot Age Gating," arXiv:2602.10251, preprint, arXiv, February 10, 2026, https://doi.org/10.48550/arXiv.2602.10251.

We recommend adding a requirement that covered businesses share documentation with the Attorney General and make a version of the documentation publicly available.

B. Covered businesses should obtain annual certification of their age assurance systems from an accredited third-party evaluator.

Public disclosure of company assessments is helpful in establishing transparency and supporting accountability; however, it is not a substitute for independent review. KGI's analysis of companies' systemic risk assessments under the European Union's Digital Services Act (DSA) illustrates the limitations of relying on company self-assessment alone. Where companies are not subject to sufficiently detailed evaluation and documentation requirements or meaningful independent scrutiny, their disclosures may remain too high-level to allow outside stakeholders to assess the rigor of the underlying analysis, the adequacy of identified mitigations, or the basis for key judgments.[9]

The proposed Rule presents a similar concern. It relies on covered businesses to evaluate their own age assurance systems and document their own compliance. Although the Rule imposes additional obligations when businesses rely on third-party age assurance providers, it does not require an independent party to evaluate or certify the covered business's compliance. The Rule should require a competent, independent evaluator — that is, an accredited third party — to review and certify the covered business's comprehensive assessment.

That review should extend beyond verifying the accuracy of reported performance results or confirming that required documentation exists. The accredited third party should scrutinize the full set of considerations and system features the covered business is required to assess and document under the Compliance and Oversight section, including whether the business used reasonable assessment methods, accurately characterized relevant risks and limitations, and reached reasonable conclusions about method selection, escalation, system design, vendor dependencies, and appropriate safeguards.

The results of the certification process should also be made public alongside the covered business's own documentation, subject to the same narrowly tailored protections for sensitive information.

We recommend requiring covered businesses to undergo an evaluation and certification by an accredited third party at least annually to assess compliance with the requirements of the proposed Rule. We also recommend that the results of this process be provided to the Attorney General and be made publicly available on the covered business's website.

[9] Peter Chapman and Matt Steinberg, *Measuring Risk: What EU Risk Assessments and US Litigation Reveal About Meta and TikTok* (2026), https://kgi.georgetown.edu/research-and-commentary/measuring-risk-what-eu-risk-assessments-and-us-litigation-reveal-about-meta-and-tiktok/.

C. Recommended changes to proposed Rule text

We suggest the changes below to effectuate the recommendations made throughout Section VI.

In the Definitions section, add:

> **"Accredited third party" means a person recognized by the American National Standards Institute (ANSI) or equivalent accreditation body, in accordance with a recognized industry standard, as qualified to certify an age assurance method. The accredited third party must be independent of the covered business and any provider whose age assurance process or technique is being evaluated and must possess appropriate technical expertise to assess the age assurance system and compliance with this Rule.**

In the Compliance and Oversight section, add:

> **Reporting requirements.**
>
> 1. **A covered business shall make publicly available an accessible, up-to-date version of the documentation required under this section describing its age assurance system and the assessment conducted pursuant to this Rule.**
> 2. **A covered business may redact specific information from the public version of the documentation only where its disclosure would materially facilitate circumvention, or risk exposing otherwise sensitive information. Any redaction shall be narrowly tailored, and the public documentation shall describe the nature of the redacted information and the basis for withholding it.**
> 3. **The covered business shall provide the Office of the Attorney General, upon request and after any reassessment, with the complete, unredacted documentation required under this section.**
> 4. **Public documentation shall be updated following any material change to the age assurance system and at least as frequently as the periodic reassessment required under this Rule.**
>
> **Independent Evaluation and Certification.**
>
> 1. **A covered business shall obtain, at least annually, an evaluation and certification of its age assurance system and the assessment and documentation required under this section from an accredited third party.**
> 2. **The accredited third party shall review the complete, unredacted assessment and documentation required under this section and evaluate whether the covered business's assessment methods, findings, conclusions, and implementation decisions are reasonable, adequately supported, and consistent with the requirements of this Rule.**

3. **The accredited third party shall conduct any additional testing or analysis necessary to substantiate the covered business's reported results or conclusions rather than relying solely on representations or documentation supplied by the covered business. The covered business shall provide the accredited third party with sufficient access to the underlying systems and data to facilitate such testing.**
4. **The accredited third party shall issue a written certification report describing the scope and methods of its review, any material limitations on the review, any identified deficiencies, and its determination as to whether the covered business complies with this Rule.**
5. **A covered business shall provide the complete certification report to the Office of the Attorney General and shall publish a public version of the report. Information may be redacted from the public version only where its disclosure would materially facilitate circumvention, or otherwise risk exposing sensitive information. Any redaction shall be narrowly tailored.**
6. **A covered business shall obtain a new accredited third party and certification following any modification to its age assurance system that could materially affect its performance, risks, or compliance with this Rule.**

VII. Appendix

As discussed in Section II(C), in each of the provisions below, "covered minor" should be replaced with "consumer."

- CP ___ Applicability (a): It adopts a flexible, proportionate framework to protect ~~covered minors~~ **consumers** and minimize privacy concerns.
- CP ___ Definitions (f): Credential-based age assurance" means an age assurance process or technique that relies on documentation, identity records, authoritative records, or third-party validation to determine, confirm, or support a ~~covered minor's~~ **consumer's** age or age range.
- CP ___ Definitions (i): 'Highly intrusive age assurance' means an age assurance process or technique that involves the collection or processing of biometric data, identity documentation, persistent identifiers, sensitive personal data, or other data practices that create a significant risk of linkability to a ~~covered minor~~ **consumer**.
- CP___ Definitions (j): 'Linkability' means the ability to associate a ~~covered minor~~ **consumer** across services, sessions, or contexts, whether directly or indirectly.
- CP___ Definitions
  - (k) 2. ii: Accessibility and ease of use for ~~covered minors~~ **consumers**
  - (k) 2. iii: The burden imposed on ~~covered minors~~ **consumers**;
- CP ___ Accuracy and Error Evaluation
  - (c): A covered business shall not use an age assurance process or technique where the error rate creates a material risk of misclassification of ~~covered minors~~ **consumers**.

    - (d) 1. Disproportionately affect certain ~~covered minors~~ **consumers** or groups of ~~covered minors~~ **consumers**;
    - (d) 2: Result in systematic under-classification or over-classification of ~~covered minors~~ **consumers**.
    - (d) 3: Result in materially disproportionate error rates, accessibility barriers, or adverse outcomes for certain ~~covered minors~~ **consumers** or groups of ~~covered minors~~ consumers."
- CP __ Frequency and Reassessment
    - (a): A covered business shall not conduct age assurance relating to a ~~covered minor~~ **consumer** more frequently than reasonably necessary to achieve the reasonably necessary level of accuracy or confidence for the applicable online service, product, or feature.
    - (b) 4: Require reverification in a manner that creates unnecessary burden, friction, or repeated collection of personal data from a ~~covered minor~~ **consumer**.
    - (d): In determining whether the frequency of age assurance or reverification for a ~~covered minor~~ **consumer** is reasonably necessary, the Attorney General may consider: [...]
    - (e): Age assurance practices that involve persistent monitoring, repeated collection of personal data, or continuous reassessment of a ~~covered minor's~~ **consumer's** age-related status shall be presumed disproportionate unless the covered business demonstrates, through clear and convincing evidence, that such practices are strictly necessary to address a reasonably foreseeable risk of material privacy, safety, or accessibility harms to covered minors."[10]
- CP __ Data Minimization in Age Assurance
    - (e) A covered business shall not retain or use age assurance data in a manner that enables tracking, profiling, behavioral advertising, or cross-service identification of a ~~covered minor~~ **consumer.**
- CP __ Linkability and System Design
    - (a) A covered business shall design and implement age assurance systems to minimize the risk of linkability to a ~~covered minors~~ **consumer** across services, devices, accounts, or contexts.
    - (b) 2: Use persistent identifiers or other techniques that enable cross-service, cross-context, or cross-device tracking of a ~~covered minor~~ **consumer**
- CP __ Prohibited Uses, Retention, and Disclosure of Age Assurance Data
    - (b) 2: Use age assurance data to build, enhance, or supplement profiles relating to ~~covered minors~~ **consumers**.
    - (b) 3: Use age assurance data to infer additional characteristics, behaviors, or preferences of a ~~covered minor~~ **consumer.**

[10] Note that in this instance, we highlight the first use of "covered minor" because requirements to not track users should apply regardless of age status. We do not highlight the second use of "covered minor" because that use pertains to the specific harms of the covered business's product to minors.

- CP __ Fallback and Accessibility
    - (b): A ~~covered minor~~ **consumer** should not be denied access to an online service, product or feature solely because [...]
    - (b) 2: A ~~covered minor~~ **consumer** declines or is unable to use a highly intrusive age assurance process or technique where less intrusive alternatives are reasonably available
    - (c) 4: Be reasonably accessible and usable by ~~covered minors~~ **consumers**.
    - (c) 6: Be designed to accommodate accessibility needs and technological limitations reasonably foreseeable and for ~~covered minors~~ **consumers**.
    - (d): A covered business shall not design fallback mechanisms in a manner that materially discourages, delays, or interferes with the use of a lower-intrusion age assurance alternative for a ~~covered minor~~ **consumer**.
- CP __ Appeals Process
    - (b) 2: Provide a meaningful opportunity for a ~~covered minor~~ **consumer** to challenge, correct, or supplement an age-related determination
    - (b) 3: Be reasonably accessible and usable by ~~covered minors~~ **consumers**.
    - (d): A reviewer shall consider information reasonably provided by the ~~covered minor~~ **consumer** in support of the appeal
    - (e) 2: Not require a ~~covered minor~~ **consumer** to provide unnecessary additional data
    - (g): ~~Covered minors~~ **Consumers** shall receive clear, understandable explanations of appeal outcomes, including any resulting correction, modification, or denial.
    - (h): A covered business shall provide an alternative age assurance process or technique for a ~~covered minor~~ c**consumer** during the appeals process where reasonably available
    - (i): A covered business shall not penalize, disadvantage, delay, restrict, or otherwise interfere with a ~~covered minor~~ **consumer** for submitting or pursuing an appeal.
    - (k): A covered business shall not design or implement age assurance processes or techniques in a manner that foreseeably results in materially disproportionate barriers, burdens, or error rates for certain ~~covered minors~~ consumers or groups of ~~covered minors~~ consumers."
- CP __ Compliance and Oversight
    - (e): Ongoing review: A business shall periodically review and update age assurance processes, techniques, and assessments to address changes in technology, risks, error rates, accessibility impacts, or reasonably foreseeable harms to ~~covered minors~~ **consumers**.

VIII. References

Chapman, Peter, and Matt Steinberg. *Measuring Risk: What EU Risk Assessments and US Litigation Reveal About Meta and TikTok*. 2026. https://kgi.georgetown.edu/research-and-commentary/measuring-risk-what-eu-risk-assessments-and-us-litigation-reveal-about-meta-and-tiktok.

Figueira, Olivia, Pranathi Chamarthi, Tu Le, and Athina Markopoulou. "Actions Speak Louder Than Chats: Investigating AI Chatbot Age Gating." arXiv:2602.10251. Preprint, arXiv, February 10, 2026. https://doi.org/10.48550/arXiv.2602.10251.

Grother, Patrick J., Mei Lee Ngan, Joyce Yang, George W. Quinn, and Austin Hom. *Face Analysis Technology Evaluation: Age Estimation and Verification*. NIST IR 8525. National Institute of Standards and Technology (U.S.), 2024. https://doi.org/10.6028/NIST.IR.8525.

Minocha, Shreyas, Isaac Sheridan, Harry Oppenheimer, Paul Pearce, and Michael A. Specter. "Papers, Please: A First Look at Age Verification on the Web." *2026 IEEE Symposium on Security and Privacy (SP)*, May 2026, 4185–202. https://doi.org/10.1109/SP63933.2026.00161.

New York Attorney General. "SAFE for Kids Act Implementing Rules." July 28, 2026. https://ag.ny.gov/safe-for-kids-act-final-rule.

Rescorla, Eric, Zander Arnao, and Alissa Cooper. *Age Assurance Online: A Technical Assessment of Current Systems and Their Limitations*. Knight-Georgetown Institute, 2026. https://kgi.georgetown.edu/research-and-commentary/age-assurance-online.

Winecoff, Amy, and Miranda Bogen. "Improving Governance Outcomes Through AI Documentation: Bridging Theory and Practice." *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, April 26, 2025, 1–18. https://doi.org/10.1145/3706598.3713814.

Winecoff, Amy, and Alissa Cooper. *Age Assurance Rules: An Implementation Guide*. 2026. https://kgi.georgetown.edu/research-and-commentary/age-assurance-rules-implementation.

Bambara, Anthony

Subject: Comment on proposed rule, 9 V.S.A. § 2449f (Prohibited Data and Design Practices)

From: Felix Parey <hello@picobellosoftware.com>
Sent: Friday, 25 September 2026 09:07:01
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: Comment on proposed rule, 9 V.S.A. § 2449f (Prohibited Data and Design Practices)

Some people who received this message don't often get email from hello@picobellosoftware.com. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Dear Attorney General,

Please find attached the comments of Picobello Software UG (haftungsbeschränkt) on the proposed Consumer Protection Rule under 9 V.S.A. § 2449f, final draft dated July 8, 2026.

Kind regards,

Felix Parey
Managing Director

Picobello Software UG (haftungsbeschränkt)
c/o The Base Berlin One · Pestalozzistraße 5-8, Apt. 216 · 13187 Berlin, Germany
Phone +49 160 93115625 · hello@picobellosoftware.com · picobelloapp.com

Picobello Software UG (haftungsbeschränkt) · Registered office: Berlin
Commercial register: Amtsgericht Charlottenburg, HRB 291439 B
Managing Director: Felix Parey

Picobello Software UG (haftungsbeschränkt)
c/o The Base Berlin One
Pestalozzistraße 5-8, Apt. 216
13187 Berlin, Germany
hello@picobellosoftware.com · picobelloapp.com

Office of the Attorney General
Consumer Protection Unit
109 State Street
Montpelier, VT 05609
United States
By email: ago.rulemaking@vermont.gov

Berlin, September 25, 2026

Re: Comments on the proposed Consumer Protection Rule under 9 V.S.A. § 2449f, "Prohibited Data and Design Practices" (final draft dated July 8, 2026)

Dear Attorney General,

Picobello Software UG is a small company in Berlin, Germany. We make Picobello, a family chore app for iOS and Android. Parents choose household chores ("quests") and rewards from a curated list. Children complete the chores in the real world and earn a fixed number of in-app coins for each one. They exchange those coins for rewards their parents define, such as extra reading time or a trip to the park. Coins cannot be bought. The app has no advertising, no messaging, no user-generated content, no feeds and no public profiles. A parent approves every child profile before it can be used.

We support the Rule's aims, including the overnight limit on push notifications. We write because three provisions, as drafted, could be read to prohibit features that serve the opposite purpose to the engagement-maximizing designs the Rule targets. Our product exists to move children away from the screen and toward tasks their parents have chosen.

1. Reinforcement Mechanisms — fixed rewards for completing an offline task

The section prohibits "variable or intermittent rewards to influence engagement by a covered minor" and lists "Likes, badges, or points" and "Gamified incentives" as illustrative examples. The operative standard, variable or intermittent rewards, targets unpredictable reward schedules. The examples, read alone, could reach any points system, including a fixed one.

We ask the Attorney General to state that a reward is not "variable or intermittent" where (a) its amount and the action that earns it are fixed and disclosed in advance, (b) it is earned by completing an activity performed outside the online service, and (c) a parent or guardian has chosen the activity and the reward. A sticker chart on a refrigerator does not become harmful because it is kept in an app. One option is a new subsection: "This section does not prohibit predetermined rewards, disclosed in advance, that are earned by completing an offline activity selected by the covered minor's parent or guardian."

2. Social Pressure Features — repeated offline activity is not engagement

The examples include "Streaks or other features that reward continuous or repeated engagement." Household routines repeat by nature: a child makes the bed every day. We ask the Attorney General to state that "engagement" in this section means engagement with the online service, product or feature.

On that reading, a feature that records the completion of recurring offline activities is not a streak unless it rewards continuous use of the service itself, or penalizes the minor for missing a period of use.

3. Push Notifications — parent-configured and task-deadline notices

The exceptions in subsection (e) cover notifications "expressly requested by a covered minor" and those "necessary to provide an online service, product, or feature in direct response to an express and unambiguous request by a covered minor." In a family product, a parent often sets up a notification for a child, for example a reminder that a chore the child accepted is due soon.

We ask the Attorney General to (a) extend these exceptions to notifications that a parent or guardian of the covered minor has requested or configured, and (b) confirm that a single notice about the deadline of a task the minor chose to accept is sent "in direct response to an express and unambiguous request" by the minor. We do not ask for any change to the 12:00 a.m. to 6:00 a.m. restriction in subsection (d).

These clarifications would keep the Rule's protections against engagement-maximizing design in full, while leaving room for tools that help parents and children organize family life away from the screen.

Thank you for considering these comments. We are glad to provide any further information.

Sincerely,



Felix Parey
Managing Director
Picobello Software UG (haftungsbeschränkt)

Bambara, Anthony

Subject: Public Comment on Proposed Rule 26P027
Attachments: Vermont Public Comment - Herscovitch.docx (1).pdf

From: Brandon Herscovitch <brandonherscovitch@gmail.com>
Sent: Sunday, 27 September 2026 13:09:21
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: Public Comment on Proposed Rule 26P027

Some people who received this message don't often get email from brandonherscovitch@gmail.com. Learn why this is important
EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Hello,

Please find attached my public comment on Proposed Rule 26P027, Prohibited Data and Design Practices. Thank you for considering it.

Brandon

Brandon Herscovitch, PhD, BCBA-D

September 27, 2026

To: Office of the Vermont Attorney General

Re: Proposed Rule 26P027, Prohibited Data and Design Practices

I am a doctoral-level behavior analyst. I support Vermont's goal of protecting minors from online design practices that may contribute to compulsive use. I offer these comments to help identify what practices the rule addresses, what effects matter, and how Vermont can evaluate and refine its protections.

1. Define the behavior and design feature the rule addresses.

The draft prohibits "variable or intermittent rewards" and gives likes, badges, points, intermittent feedback systems, and gamified incentives as examples (draft p. 12). A reward is something offered, such as a badge. A reinforcer is a consequence shown to increase or maintain the future occurrence of a particular action. Whether a badge functions as a reinforcer must be determined from its effect on behavior. At the same time, a minor might continue scrolling because some of the content presented in a feed is more engaging to that minor than other content, even though the draft does not call content a reward. These consequences also differ in who produces them. Likes and comments come from other users. Badges and points are awarded by the business, and the business selects the content in the feed using its algorithms, rules, and data on user behavior. The business decides when to award badges and points, how and when to display peer feedback, and how to select and present feed content. These are not mere technicalities. A business could remove badges and comply with this provision while continuing to select and present feed content in ways that sustain prolonged use and may contribute to harm. The draft addresses personalized feeds elsewhere, but that does not clarify what this provision means by "rewards."

The answer is not to prohibit all variable or intermittent outcomes. A functioning social media feed presents changing content, some of which may reinforce continued use. That variability is part of how feeds work. The Act provides that the content of media a minor views shall not establish compulsive use (9 V.S.A. § 2449c(c)). The concern is how content is selected and delivered, and what effects follow. To address its effects, Vermont might consider examining both explicit rewards, such as badges, and how platforms arrange the selection, order, and timing of what they deliver: what users do, what follows, how delivery varies, and whether these arrangements maintain use or contribute to harm. This would let the rule target consequential design choices without treating variability, intermittence, or company-programmed rewards as a sufficient account of the reinforcement mechanisms it aims to address.

I encourage the Attorney General to identify the action at issue, such as returning to an app or continuing to scroll; the feature the business controls, such as how items are ordered, how often new items appear, and when they are delivered; and the effects that warrant investigation. Vermont could then compare behavior when a specified feature is present, changed, or removed, rather than treating the label "reward" or the presence of variability as proof of reinforcement or harm. This would give businesses clearer direction and help Vermont evaluate the protections it adopts.

2. Measure the outcome Vermont is trying to prevent.

Once Vermont identifies a feature or features that change use, it may be well served to ask what that change means for the minor. A feed change might lead to longer sessions, but longer sessions alone do not

establish compulsive use. The Act defines compulsive use in terms of repetitive use that materially disrupts a minor's major life activities (9 V.S.A. § 2449a(8)).

The draft treats increased engagement as evidence that a practice leads to compulsive use (draft pp. 7-8). I encourage the Attorney General to use increased time or app openings as reasons to investigate, and also examine whether use is linked to meaningful effects on the major life activities the Act names, such as sleeping, learning, and communicating, as well as on anxiety or well-being. Whether minors keep using a service after deciding to stop and their accounts of what they intended and experienced may also be informative. Findings about these outcomes should be assessed carefully before attributing them to a particular feature.

3. Use the required review to test and refine the rule.

The Act requires the Attorney General to review these rules at least every two years and update them as necessary (9 V.S.A. § 2449f(b)). That review can ask whether a regulated feature changed the behavior identified above and whether the change was linked to the outcomes Vermont seeks to protect.

I encourage Vermont to record what feature changed and when, define the measures before assessing results, and check that the data accurately capture what they claim to measure. Where feasible, comparisons should account for other changes that could explain the results. No single study design will answer every question: group comparisons can estimate broader effects, repeated measurement of individuals can reveal differences across minors and circumstances, and minors' own accounts provide another source of information. The review can then identify which provisions to keep, revise, or test further. This gives Vermont a way to act now and improve the rule as evidence develops.

I would welcome the opportunity to provide proposed language or help identify measures for evaluating these provisions. My aim is to make the rule technically accurate, understandable, and effective in protecting minors.

Brandon Herscovitch, PhD, BCBA-D

brandonherscovitch@gmail.com

Sources

Proposed rule, Prohibited Data and Design Practices, draft pp. 7-8, 12:
https://ago.vermont.gov/vermont-age-appropriate-design-code-rulemaking

9 V.S.A. § 2449a(8), definition of compulsive use:
https://legislature.vermont.gov/statutes/section/09/062/02449a

9 V.S.A. § 2449f(b), rulemaking and review:
https://legislature.vermont.gov/statutes/section/09/062/02449f

9 V.S.A. § 2449c(c), content of media:

https://legislature.vermont.gov/statutes/section/09/062/02449c

Bambara, Anthony

From: Jameson, Sarah
Sent: Tuesday, September 29, 2026 12:10 PM
To: Bambara, Anthony
Subject: Fw: Solid Rules

Get Outlook for iOS

From: Anne Kaplan <anne3kaps@gmail.com>
Sent: Monday, 28 September 2026 17:35:57
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: Solid Rules

Some people who received this message don't often get email from anne3kaps@gmail.com. Learn why this is important
EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

The rules for age appropriate design code seem very thorough. How are websites or apps going to figure out whether an adult or a minor is using their site? How will the state be checking to make sure companies are following these rules? I appreciate the hard work everyone is doing to protect Vermonters from the whims and profit seeking companies that want to monopolize our attention, time, and money. Thank you.

--
Anne Kaplan
She/Her
802-355-0955

Bambara, Anthony

From: Jameson, Sarah
Sent: Tuesday, September 29, 2026 12:10 PM
To: Bambara, Anthony
Subject: Fw: Written comment to rule change on technology use and minors

Forwarding comments to post to the rulemaking page. Thanks!

Get Outlook for iOS

From: Colleen Kutin <clumpykut@yahoo.com>
Sent: Monday, 28 September 2026 23:28:03
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: Written comment to rule change on technology use and minors

Some people who received this message don't often get email from clumpykut@yahoo.com. Learn why this is important
EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

As a mental health practitioner of minors that has worked in the field over 25 years , i strongly support new rules around limiting access and adding restrictions to technology for minors.
I see firsthand in my work the effects it has on children and families .

I fully support the ideas you present in your slide show.

Three items i am not sure i saw you address, which i find to be a problem with the children and families are:

1) the marketing of online games and products
It seems this can be done by ads, but also by people posting reels and YouTube videos and by influencers
Kids see it over and over and then it becomes something that they need
And they obsess over so to fit in, and then they want to spend large amounts of money and energy on getting them
And often a quick fad, like the recent neehdoh obsession happens

2)scary, often AI content
I have had a handful of kids show up in my office who were on kids YouTube, or instagram or Snapchat and some sort of reel/video comes up that has content that is scary(most often not real)
One example is this past year, someone was posting about a animatronic he was building that was coming to life (a sort of the FNAF like character), and it was to roam the world haunting people
The videos actually showed the process with the animatronic and new videos continued to pop into this childs feed over some months showing the process of the project , even through she and her parents tried to get them to stop and avoid them
Her final solution was no technology usage

3) make games have some sort of age restriction if they make users pay money to continue playing or gain rewards
Or make games not make users pay money in general (its not healthy for adults either)

Example: there are many games available on the internet that one can play
You start playing for free, then they begin to ask for money to continue to play, or more frequently they let you play for free but to do well in the game, to earn rewards in the game, or buy extra lives, or get some sort of benefit in the game you must pay real money
Some of them are like gambling games of sorts
They draw the kids in, then they are buying things on the phone and obsessing about getting rewards etc
It like a bit like a gambling addiction

I see kids coming in my office with sleep issues, anxiety, panic attacks and fear/worry related to the above issues
Additionally, it causes family issues as parents are trying to navigate boundaries and help their kids stay safe and well.

Thanks for all you are doing
Colleen kutin

If you are experiencing a mental health emergency, please call 988 or go to your nearest emergency room

24-hour Hotlines:
Northeast Kingdom Human Services
24-Hour Emergency: 1-(802)-334-6744(Derby)
1-(802)-748-3181 (St. Johnsbury)
Lamoille County Mental Health Services

Crisis: 1-(802)-888-5026 Mon.-Friday
1-(802)-888-8888 Nights & Weekends
Washington County Mental Health

Website: http://www.wchs.org/
24-hour Emergency : 1-(802)-229-0591
National Suicide Prevention Hotline: 1-800-273-TALK (8255)

Crisis Text Line: Text 741741 from anywhere in the US to text with a trained Crisis Counselor.

STATEMENT OF CONFIDENTIALITY
The information contained in this electronic message and any attachments may contain confidential or privileged information intended for the exclusive use of the addressee(s). If you are not the intended recipient, please notify the sender by reply email and destroy all copies of the original message and any attachments. In accordance with Electronic Communications Privacy Act, 18 USC&&2510-2521

Bambara, Anthony

From: Jameson, Sarah
Sent: Tuesday, September 29, 2026 12:11 PM
To: Bambara, Anthony
Subject: Fw: Public Comment on Sections 2249f and 2449g of Act 63

Get Outlook for iOS

From: Case <cgriffingjr@protonmail.com>
Sent: Monday, 28 September 2026 15:45:41
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: Public Comment on Sections 2249f and 2449g of Act 63

Some people who received this message don't often get email from cgriffingjr@protonmail.com.
Learn why this is important
EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

I do not consent to the State of Vermont directing private corporations to determine my age in its rules pursuant to 9 V.S.A. 2449g:

> (c) A covered business shall implement proportionate age assurance measures for any online service, product, or feature reasonably likely to be accessed by covered minors.
>
> (d) A covered business shall determine whether a user is a covered minor using a proportionate age assurance method.

This is a violation of my privacy. It's bad enough that web sites and services invasively surveil users, build profiles on us, and sell our data back and forth to one another like private intelligence agencies. I don't appreciate that my state government is *telling* them to do it.

I agree that we need to protect children from this predatorial behavior. But instead of protecting them by putting the rest of us at risk, protect the online privacy of ALL Vermonters.

Sincerely,

Charles Griffing, Jr.
Shrewsbury, Vermont

Bambara, Anthony

Subject: Comment on the proposed Age Assurance Privacy rule (9 V.S.A. § 2449g)

From: Cison LLC <legal@cison.net>
Sent: Wednesday, 30 September 2026 00:15:54
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: Comment on the proposed Age Assurance Privacy rule (9 V.S.A. § 2449g)

Some people who received this message don't often get email from legal@cison.net. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Cison LLC is building Cison, a small social network based in North Carolina. It isn't open to the public yet, and it intends to serve people 13 and older in the United States. In Cison's design, every account for someone 13 to 17 is tied to a guardian: an adult with their own account who agrees to look after the young person's account. Before a guardian's first sign-off, Cison asks them to pass a one-time identity check with a vendor (a government ID and a live selfie). The check confirms that the guardian is a real, specific adult. It exists to stop a minor from approving their own account, and to stop one person from holding guardian roles under several identities.

We support the proposed rule's framework. We ask the Attorney General to address one question the draft leaves open.

The rule defines age assurance as any process "used to determine, estimate, or communicate the age or age range of a user, including whether a user is a covered minor." Verifying a parent or guardian, so that their consent is real, includes confirming that the adult is not a minor. Read literally, every guardian verification would then be "credential-based" or "highly intrusive" age assurance, subject to graduated escalation, a lower-intrusion fallback, and the presumption in Compliance and Oversight (h).

We ask that the final rule, or the Attorney General's guidance, state that:

1. verifying the identity and adulthood of a parent or guardian, in order to obtain or confirm consent for a covered minor, is not age assurance of the covered minor under this rule; and
2. the methods of verifiable parental consent recognized in the federal COPPA rule (16 C.F.R. § 312.5(b)(2)), including a government ID checked against a live photo and a payment-card transaction, are proportionate for that purpose.

A guardian's verification answers a different question from age assurance. It doesn't ask "is this user a minor?" It asks "is this adult who they say they are, and entitled to act for this minor?" Lower-intrusion methods such as self-declaration, estimation or account signals can suggest that someone is probably an adult. They can't establish a specific adult's identity, which is what makes consent meaningful and what stops a minor, or someone with bad intentions, from posing as a parent. Other states require this kind of parental verification and then its deletion (for example Tenn. Code Ann. § 47-18-5703 and Mississippi H.B. 1126 (2024), § 4(2)(d)). A clear statement would let a business meet those laws and Vermont's rule with one design.

The minor's own age remains subject to the rule. In our design the minor declares their age and a verified adult confirms it: a self-declaration combined with a safeguard, which the proposed rule lists as low-intrusion age assurance (Graduated Escalation (a)(1)(i)).

Thank you for considering this comment.

Johnny Cison
Founder and Sole Member, Cison LLC
PO Box 161, Jarvisburg, NC 27947
legal@cison.net

Bambara, Anthony

Subject: TechNet AADC Proposed Rule Comments

From: Christopher Gilrein <cgilrein@technet.org>
Sent: Thursday, 01 October 2026 14:28:27
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: TechNet AADC Proposed Rule Comments

Some people who received this message don't often get email from cgilrein@technet.org. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Thank you for the opportunity to share TechNet's comments on the proposed rules. Our letter is attached.

Thanks,
Chris

Christopher Gilrein
Executive Director | Massachusetts & Northeast
TechNet | The Voice of the Innovation Economy
(c): 774-230-6685 | cgilrein@technet.org



TECHNET
THE VOICE OF AMERICAN INNOVATION

TechNet Northeast
Boston, MA 02108
www.technet.org

October 1, 2026

The Honorable Charity Clark
Attorney General
State of Vermont

Re: Proposed rules for Sections 2249f and 2449g of Act 63

Dear Attorney General Clark:

TechNet is the national, bipartisan network of technology companies that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes 100 dynamic American businesses ranging from startups to the most iconic companies on the planet and represents five million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

TechNet strongly supports protecting children's privacy online while ensuring regulations are workable, innovation-friendly, and constitutionally sound. Our member companies have been at the forefront of raising the standard for children's safety and privacy online, investing in new features, parental tools, and settings that are age-appropriate and tailored to the differing developmental needs of young people. We offer the following feedback on the proposed rules.

Broadly speaking, TechNet believes the proposed rules exceed the office's statutory remit in key instances; expanded operative definitions that fundamentally alter the effect of the underlying legislation; and unnecessarily restrict common, pro-consumer design best practices. The following recommendations seek to ameliorate these concerns and provide clarity, rather than confusion, to the underlying legislation.

Proposed rules replace the statutory knowledge standard

Act 63 regulates business practices with regard to a "covered minor", defined therein as "a consumer the business actually knows is a minor or labels as a minor pursuant to age assurance methods in rules adopted by the Attorney General". The proposed Prohibited Data and Design Practices rule instead determines a business to "have reason to know" a user is a covered minor whenever the service is "reasonably likely to be accessed by a covered minor" – effectively replacing the Act's actual-knowledge standard with a constructive-knowledge standard, which is inconsistent with other state privacy laws and COPPA.

Within the Age Assurance Framework section, TechNet seeks clarification to align with Act 63's explicit direction to "prioritize privacy and accessibility over the accuracy of age assurance methods". The proposed rules simultaneously require businesses to (1) begin

with the least intrusive age assurance method (self-declaration) and (2) not use any method with a "material risk of misclassification". Given the high potential for misclassification inherent in self-declaration, the rules seem to mandate more intrusive methods, despite the statutes' privacy-first framing. TechNet seeks clarification that the rules do not mandate age verification or age-gating and defined "reasonable safeguards" to provide companies with a safe harbor for self-declaration.

Proposed definitions expand scope beyond legislative intent and authority

The definition of "compulsive use" in the underlying statute explicitly requires repetitive use that materially disrupts major life activities, including eating, sleeping, learning, or working. The proposed rule materially lowers this threshold by categorizing any practice that optimizes engagement, increases interaction, or lacks contemporaneous requests as inducing compulsive use.

The rules further seek to expand the scope to include standard engagement optimization by including a definition of "heightened risk of harm" that includes vague and subjective examples like "prolonged use beyond intent". Per Act 63, "material disruption" is the only valid legal standard for compulsive use and the regulations must reflect that.

Additional vague or undefined terms include: "behavioral inference", which appears once and is duplicative of the separate defined term "inferred preferences"; and "subvert or impair autonomy", the broadness of which creates significant uncertainty for developers and should be stricken or narrowed to provide a clear compliance pathway.

Act 63 intends to balance parental supervision with the covered minor's privacy and autonomy by requiring a covered business to provide a conspicuous signal when a parent, guardian, or other individual is monitoring a covered minor's activity or tracking their location. The proposed rules both change the scope of disclosure by including monitoring and tracking by a covered business as a trigger for signaling and significantly broaden the scope of activities that require signaling by expanding the definitions of "monitoring" and "tracking" beyond the statute's intent.

The net result is a signal that will effectively always be on, resulting in a continuous disruption to the minor's use of a service that will effectively fade into the background as notification fatigue sets in. TechNet suggests that the rules be amended to align with the underlying statute in applying to tracking by a covered parent, guardian, or individual, and by striking or narrowing the definitions of monitoring and tracking to focus strictly on real-time tracking, consistent with requirements in other legal frameworks.

TECHNET
THE VOICE OF AMERICAN INNOVATION

Proposed data and design restrictions exceed authority and ban necessary design features

The proposed restriction on secondary uses of data exceeds the data minimization requirements in the underlying statute. Consistent with Act 63 and Vermont's data privacy statute, TechNet suggests striking subsections (c) and (d) and including the statutory exemption "unless necessary to comply with any obligation under this chapter" in subsection (a).

Similarly, the proposed definition of "necessary to provide a service" limits data processing to what is strictly required to provide a feature and responsive to an express and unambiguous request. This would prevent platforms from providing personalization even when a covered minor explicitly enables such settings. The definition further explicitly states that certain internal, operational functions are not deemed necessary. TechNet seeks amendments to allow processing where it is strictly necessary or directly responsive to a user request, and to align operational exemptions with COPPA.

The proposed definition of "express and unambiguous request" appears to prohibit companies from arguing that user-selected account settings constitute valid requests for personalization. We seek to strike the phrase "specific and contemporaneous" and clarify that account-level personalization settings qualify as consent. TechNet seeks similar clarification in the Personalized Media section (d)(1)-(3) affirming that personalization is permissible when enabled by a user setting and that general customization is permissible when necessary to provide functional service.

Finally, TechNet asks the office to strike the proposed ban on behavioral recommendation systems. Personalized recommendation systems are essential for usability and safety. They filter harmful or spam material and adapt to different developmental needs of young people. The underlying statute imposes data and design restrictions based on compulsive use by covered minors. It does not support a blanket prohibition.

Creates a new general duty

The proposed rule prohibits covered businesses from designing or deploying practices that create a reasonably foreseeable "heightened risk of harm". Act 63 enumerates a specific set of harms business must avoid. As written, the rule would create an unauthorized expansion of the statutory mandate.

Effective date does not give adequate time for compliance

In the interest of advancing an effective compliance process for covered minors, TechNet respectfully requests that the Office announce a delayed enforcement to provide for enough time for businesses to plan, build, and deploy compliance solutions. Given the January 1, 2027 effective date, the runway to implement solutions based on the final rules will be extremely short. We ask that the AG be a partner in our shared

goal of offering a safe and operational online experience and delay enforcement for 12 months.

Thank you for your consideration.

Sincerely,



Christopher Gilrein
Executive Director, Northeast
TechNet
cgilrein@technet.org

Bambara, Anthony

Subject: SIIA Comments on VT AADC Rulemaking

From: Abigail Wilson <awilson@siia.net>
Sent: Thursday, 01 October 2026 10:54:55
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: SIIA Comments on VT AADC Rulemaking

Some people who received this message don't often get email from awilson@siia.net. Learn why this is important
EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

October 1, 2026

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

RE: Proposed Rulemaking Regarding the Vermont Age-Appropriate Design Code (AADC)
Statement of Interest

We appreciate the opportunity to share our significant concerns regarding the current proposed rule language for the Vermont Age-Appropriate Design Code (AADC). While SIIA supports protecting youth online, the rules as proposed exceed statutory intent, interfere with beneficial user features, raise serious constitutional and federal legal conflicts, and impose unworkable compliance burdens on platforms.

SIIA is the principal U.S. trade association for the software and digital information industries. Our nearly 400 members include leading companies in software, data analytics, and digital content that are deeply committed to providing safe, secure, and privacy-protective online experiences for all users, including minors.

The Proposed Rule Exceeds Statutory Authority
The proposed rules create restrictions, definitions, and enforcement mechanisms that go beyond what was authorized by the Vermont Legislature. First, the proposed rules attempt to impose a "constructive knowledge" standard, conflicting directly with the governing statute's "actual knowledge" requirement. Additionally, the rules mandate extensive pre-deployment assessments, ongoing documentation, and oversight regimes for age assurance and design practices—requirements nowhere to be found in the statute. Finally, the draft rules broaden the definition of "compulsive use" to include anything that "materially disrupts major life activities," threatening to capture standard, benign user engagement mechanisms.

Prohibition of Personalization and Recommended Content
The rules also effectively ban the prioritization of youth-friendly content by severely restricting personalization and recommendation systems. To start, data processing is restricted strictly to what is necessary to deliver a feature. Act 63 sets two related but distinct limits: collection, sale, sharing, and retention are limited to data necessary to provide the online service, product, or feature the minor is actively and knowingly using, while

data previously collected from the minor may be used only for the purpose for which it was collected. The proposed rules narrow both standards beyond what the statute permits. “Necessary to provide a service” is limited to processing that is strictly required for a specific feature, directly responsive to an express request, and unavailable through less data-intensive means. “Secondary use” expressly includes profiling, recommendations, cross-service use, advertising, and model training and applies regardless of disclosure. The rules also state that disclosure or consent does not make a secondary use permissible. This explicitly excludes personalization, content recommendations, contextual advertising, and analytics from being considered necessary functions. Furthermore, even if a minor affirmatively enables history or recommendation settings, the underlying data processing risks being classified as impermissible under the proposed rules. By classifying profiling preferences, inferences, and recommendation algorithms as non-curable secondary uses, platforms will be forced to display uncurated, non-personalized feeds. This will disrupt user navigation across digital libraries, educational tools, and media platforms. These restrictions undermine consumer autonomy, preventing young individuals from obtaining customized digital experiences even when explicitly seeking to explore emerging interests or enhance their understanding of previously accessed educational concepts.

A separate data-retention provision makes the problem more severe. It says covered-minor data “shall not be retained” for behavioral personalization, recommendation systems, engagement optimization, model training or development, and analytics not necessary to provide the service. Except for unnecessary analytics, the list does not clearly allow retaining data reasonably needed to run the disclosed service. For recommendation-based educational services, digital libraries, media catalogs, and other adaptive or model-based services, these restrictions can be incompatible with providing the service: they may allow a feature in principle while prohibiting retention of the data needed to operate, secure, evaluate, and improve it.

User Experience Disruption and Warning Fatigue

If these rules were to pass, they could degrade user experience in Vermont and introduce regulatory uncertainty. An overly broad definition of "monitoring" mandates perpetual on-screen warnings, which will numb users to legitimate safety concerns. At the same time, prohibiting design choices that make disengagement harder than engagement creates severe legal ambiguity. Beneficial functionality—such as progress alerts or profile-switching prompts—could be improperly flagged as non-compliant friction.

Constitutional and Federal Legal Conflicts

Further, the proposed rules create direct conflicts with federal statutory frameworks and established First Amendment precedent. Restrictions on algorithmic recommendations and content curation limit editorial discretion, which is protected expression under established First Amendment precedent, such as Moody v. NetChoice and Sorrell v. IMS Health. In addition, under the federal Children’s Online Privacy Protection Act (COPPA), verifiable parental consent allows data processing for minors. The proposed rules declare parental consent irrelevant, directly conflicting with federal law.

Impacts on Platform Safety, Fraud Prevention, and Age Assurance

Additionally, the rules unintentionally compromise security and safety controls integrated into digital platforms. The final rules should clearly allow processing and retention reasonably necessary to operate and protect the service, including security, fraud prevention, child safety, accessibility, integrity, debugging, reliability, analytics needed to measure performance or detect failures, and development of models used for those purposes. Restrictions on account linkability and secondary data usage prevent platforms from detecting repeat underage users who re-register after removal, or from utilizing multilayered AI tools to flag fraudulent activity. Mandating an open-ended appeals process for age determinations without allowing platforms to reject bad-faith attempts creates severe operational risks. Finally, rigid evaluation requirements for age-assurance tools discourage platforms from utilizing comprehensive, multilayered verification systems.

Overbroad Scope and Unrealistic Compliance Timeline
While intended to target social media platforms, the broad definition inadvertently captures everyday online services used by Vermonters, including transit, banking, fitness, and navigation apps. Moreover, with rulemaking scheduled to close in October and an effective date of January 1, platforms are left with an unworkably short timeframe to build out compliance structures.

Proposed Recommendations
To ensure alignment with the law and preserve effective platform functionality while protecting youth, SIIA urges the consideration of the following modifications:

1. Align Definitions with the Statutory Baseline: Revert the definitions of "compulsive use," "covered minor," and "general duty" back to the statutory text enacted by the Legislature.
2. Protect Personalization Features: Align Data Processing and Retention with Statutory Baseline. Revise “necessary to provide a service” and “secondary use” to reflect the statute’s service-necessity and original-purpose limits, and revise the separate retention provision so data may be retained when reasonably necessary for permitted recommendations, adaptive or model-based functions, analytics, safety, security, integrity, reliability, and accessibility.
3. Refine Monitoring Signals: Limit "monitoring" strictly to real-time parental or location tracking, explicitly exempting persistent identifiers and routine logging to prevent user warning fatigue.
4. Remove DPIA and Documentation Mandates: Strike unauthorized impact assessment requirements, ongoing documentation regimes, and rigid accuracy evaluation criteria for age assurance.
5. Incorporate Anti-Fraud and Safety Carve-Outs: Permit account linking for fraud detection and safety enforcement and allow platforms to deny abusive or bad-faith age-determination appeals.

Conclusion
SIIA remains committed to working alongside the Vermont Legislature to foster safe and privacy-protective online environments. However, the proposed rules as currently drafted exceed statutory boundaries, create legal conflicts, and undermine key safety and personalization functions. We appreciate your time and consideration of these comments.

Respectfully submitted,



Abigail Wilson
Director of State Policy
Software & Information Industry Association (SIIA)
859.760.7648
awilson@siia.net

October 1, 2026

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

RE: Proposed Rulemaking Regarding the Vermont Age-Appropriate Design Code (AADC)
Statement of Interest

We appreciate the opportunity to share our significant concerns regarding the current proposed rule language for the Vermont Age-Appropriate Design Code (AADC). While SIIA supports protecting youth online, the rules as proposed exceed statutory intent, interfere with beneficial user features, raise serious constitutional and federal legal conflicts, and impose unworkable compliance burdens on platforms.

SIIA is the principal U.S. trade association for the software and digital information industries. Our nearly 400 members include leading companies in software, data analytics, and digital content that are deeply committed to providing safe, secure, and privacy-protective online experiences for all users, including minors.

The Proposed Rule Exceeds Statutory Authority

The proposed rules create restrictions, definitions, and enforcement mechanisms that go beyond what was authorized by the Vermont Legislature. First, the proposed rules attempt to impose a "constructive knowledge" standard, conflicting directly with the governing statute's "actual knowledge" requirement. Additionally, the rules mandate extensive pre-deployment assessments, ongoing documentation, and oversight regimes for age assurance and design practices—requirements nowhere to be found in the statute. Finally, the draft rules broaden the definition of "compulsive use" to include anything that "materially disrupts major life activities," threatening to capture standard, benign user engagement mechanisms.

Prohibition of Personalization and Recommended Content

The rules also effectively ban the prioritization of youth-friendly content by severely restricting personalization and recommendation systems. To start, data processing is restricted strictly to what is necessary to deliver a feature. Act 63 sets two related but distinct limits: collection, sale, sharing, and retention are limited to data necessary to provide the online service, product, or feature the minor is actively and knowingly using, while data previously collected from the minor may be used only for the purpose for which it was collected. The proposed rules narrow both standards beyond what the statute permits. “Necessary to provide a service” is limited to processing that is strictly required for a specific feature, directly responsive to an express request, and unavailable through less data-intensive means. “Secondary use” expressly includes profiling, recommendations, cross-service use, advertising, and model training and applies regardless of disclosure. The rules also state that disclosure or consent does not make a secondary use permissible. This explicitly excludes personalization, content recommendations, contextual advertising, and analytics from being considered necessary functions.

Furthermore, even if a minor affirmatively enables history or recommendation settings, the underlying data processing risks being classified as impermissible under the proposed rules. By classifying profiling preferences, inferences, and recommendation algorithms as non-curable secondary uses, platforms will be forced to display uncurated, non-personalized feeds. This will disrupt user navigation across digital libraries, educational tools, and media platforms. These restrictions undermine consumer autonomy, preventing young individuals from obtaining customized digital experiences even when explicitly seeking to explore emerging interests or enhance their understanding of previously accessed educational concepts.

A separate data-retention provision makes the problem more severe. It says covered-minor data "shall not be retained" for behavioral personalization, recommendation systems, engagement optimization, model training or development, and analytics not necessary to provide the service. Except for unnecessary analytics, the list does not clearly allow retaining data reasonably needed to run the disclosed service. For recommendation-based educational services, digital libraries, media catalogs, and other adaptive or model-based services, these restrictions can be incompatible with providing the service: they may allow a feature in principle while prohibiting retention of the data needed to operate, secure, evaluate, and improve it.

User Experience Disruption and Warning Fatigue

If these rules were to pass, they could degrade user experience in Vermont and introduce regulatory uncertainty. An overly broad definition of "monitoring" mandates perpetual on-screen warnings, which will numb users to legitimate safety concerns. At the same time, prohibiting design choices that make disengagement harder than engagement creates severe legal ambiguity. Beneficial functionality—such as progress alerts or profile-switching prompts—could be improperly flagged as non-compliant friction.

Constitutional and Federal Legal Conflicts

Further, the proposed rules create direct conflicts with federal statutory frameworks and established First Amendment precedent. Restrictions on algorithmic recommendations and content curation limit editorial discretion, which is protected expression under established First Amendment precedent, such as Moody v. NetChoice and Sorrell v. IMS Health. In addition, under the federal Children's Online Privacy Protection Act (COPPA), verifiable parental consent allows data processing for minors. The proposed rules declare parental consent irrelevant, directly conflicting with federal law.

Impacts on Platform Safety, Fraud Prevention, and Age Assurance

Additionally, the rules unintentionally compromise security and safety controls integrated into digital platforms. The final rules should clearly allow processing and retention reasonably necessary to operate and protect the service, including security, fraud prevention, child safety, accessibility, integrity, debugging, reliability, analytics needed to measure performance or detect failures, and development of models used for those purposes. Restrictions on account linkability and secondary data usage prevent platforms from detecting repeat underage users who re-register after removal, or from utilizing multilayered AI tools to flag fraudulent activity. Mandating an open-ended appeals process for age determinations without allowing platforms to reject bad-faith attempts creates severe operational risks. Finally, rigid evaluation requirements for age-assurance tools discourage platforms from utilizing

comprehensive, multilayered verification systems.

Overbroad Scope and Unrealistic Compliance Timeline

While intended to target social media platforms, the broad definition inadvertently captures everyday online services used by Vermonters, including transit, banking, fitness, and navigation apps. Moreover, with rulemaking scheduled to close in October and an effective date of January 1, platforms are left with an unworkably short timeframe to build out compliance structures.

Proposed Recommendations

To ensure alignment with the law and preserve effective platform functionality while protecting youth, SIIA urges the consideration of the following modifications:

1. Align Definitions with the Statutory Baseline: Revert the definitions of "compulsive use," "covered minor," and "general duty" back to the statutory text enacted by the Legislature.
2. Protect Personalization Features: Align Data Processing and Retention with Statutory Baseline. Revise “necessary to provide a service” and “secondary use” to reflect the statute’s service-necessity and original-purpose limits, and revise the separate retention provision so data may be retained when reasonably necessary for permitted recommendations, adaptive or model-based functions, analytics, safety, security, integrity, reliability, and accessibility.
3. Refine Monitoring Signals: Limit "monitoring" strictly to real-time parental or location tracking, explicitly exempting persistent identifiers and routine logging to prevent user warning fatigue.
4. Remove DPIA and Documentation Mandates: Strike unauthorized impact assessment requirements, ongoing documentation regimes, and rigid accuracy evaluation criteria for age assurance.
5. Incorporate Anti-Fraud and Safety Carve-Outs: Permit account linking for fraud detection and safety enforcement, and allow platforms to deny abusive or bad-faith age-determination appeals.

Conclusion

SIIA remains committed to working alongside the Vermont Legislature to foster safe and privacy-protective online environments. However, the proposed rules as currently drafted exceed statutory boundaries, create legal conflicts, and undermine key safety and personalization functions. We appreciate your time and consideration of these comments.

Respectfully submitted,



Abigail Wilson
Director of State Policy
Software & Information Industry Association (SIIA)

Bambara, Anthony

Subject: AADC Draft Rules - Motion Picture Association Comments

From: Banuelos, Kathy <Kathy_Banuelos@motionpictures.org>
Sent: Thursday, 01 October 2026 11:19:01
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: AADC Draft Rules - Motion Picture Association Comments

Some people who received this message don't often get email from kathy_banuelos@motionpictures.org. Learn why this is important
EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

To whom it may concern:
On behalf of the Motion Picture Association, attached please find our comments on the AADC draft rules. We are available to answer any questions or discuss our comments in more detail.

Respectfully,

Kathy Bañuelos
Senior Vice President
State Government Affairs
Motion Picture Association
+1 818 325 9467 (mobile)
+1 818 935 5850 (office)
kathy_banuelos@motionpictures.org

Moving Pictures. Moving Audiences. Moving Forward.

CONFIDENTIALITY NOTICE: This e-mail communication and any attachments may contain confidential and privileged information for the use of the designated recipients named above. If you are not the intended recipient, you are hereby notified that you have received this communication in error and that any review, disclosure, dissemination, distribution or copying of it or its contents is strictly prohibited. If you have received this communication in error, please notify the sender by return e-mail and delete and/or destroy all copies of this communication and any attachments.

MOTION PICTURE ASSOCIATION

October 2, 2026

The Honorable Charity R. Clark
109 State St.
Montpelier, VT 05609

Re: MPA Comments on Proposed Rules for Sections 2449f and 2449g of Act 63, An Act Relating to an Age-Appropriate Design Code

Dear Attorney General Clark:

The Motion Picture Association, Inc. ("MPA")[1] respectfully submits this letter in response to the proposed rules for Sections 2449f ("Consumer Protection Rules" or "CP Rules") and 2449g ("Age Assurance Rules" or "AA Rules," and together with the CP Rules, the "Draft Rules"), which have been drafted pursuant to Act 63, the Vermont Age Appropriate Design Code ("AADC Law").

MPA appreciates the concerns that animated the legislature's enactment of Act 63, particularly the importance of providing minors with age-appropriate and safe experiences online. However, the Draft Rules are overbroad and extend well beyond what is contemplated under the AADC Law. As written, the Draft Rules could substantially impair the ability of paid video streaming services operated by MPA's members to provide functional services to minors. Notably, the Draft Rules jettison statutory exemptions that permit streaming platforms to make recommendations to minors, expand the scope of data covered by the law's restrictions, and so narrowly define user requests that services may not be able to rely on account settings established by parents to ensure their children are only able to access age-appropriate content.

Underlying these overbroad restrictions are determinations and rules that far exceed the contemplated statutory authority. The AADC Law directs the Attorney General to draft rules to prohibit design and data practices that lead to "compulsive use" or would "impair autonomy." The CP Rules go beyond this directive, restricting practices based only on a determination that they increase engagement, effectively redefining "compulsive use," and incorporating provisions and standards that are not design or data practices. Additionally, the rules appear to conflate content-discovery mechanisms (like the home page on a streaming service) with content-consumption mechanisms (like a social media feed)—even though these services are distinct and pose fundamentally different risks.

[1] The MPA is a not-for-profit trade association founded in 1922 to address issues of concern to the motion picture industry. Since that time, MPA has advanced the business and art of storytelling, protecting the creative and artistic freedoms of storytellers, and bringing entertainment and inspiration to audiences worldwide. The MPA's members are: Amazon Studios, LLC, Netflix Studios, LLC, Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Universal City Studios LLC, Walt Disney Studios Motion Pictures, and Warner Bros. Entertainment Inc.

To address these concerns, MPA respectfully requests that the Draft Rules be narrowed to align with the AADC Law, including as described below. Additionally, in light of the numerous novel and substantial obligations contemplated by the Draft Rules, many of which far exceed any existing requirement in state or federal law, covered businesses require additional time to develop compliance procedures. Accordingly, the effective date for these novel requirements should be delayed to provide covered businesses with adequate time to develop the requisite systems and processes.

MPA Members' Streaming Services Offer a Model for Age-Appropriate Online Experiences

MPA's members operate the premier video streaming services in the world, which offer industry-leading tools to provide safe online experiences for children. A cornerstone of this framework is the MPA rating system for motion pictures, which involves human review of content before it is made available to general audiences.[2] This system serves as a model for the television rating system.[3] MPA members' video streaming services couple these ratings with robust parental controls that permit parents to determine what their children are watching, typically by creating special "kids' profiles" and restricting access to parents' profiles with a PIN.[4] To access any of these services, the primary account holder must be an adult, which means whether a child has access to the service is a determination made by the parent.

The paid streaming service model is fundamentally different from user-generated content platforms, including social media websites. Content on paid video streaming services is carefully vetted by multiple layers of human review, and access is protected with registration requirements and parental controls. By contrast, social media services and other free platforms provide access to content uploaded by millions of individual users, which appears instantly on the platform and is made available to users (including children). The walled garden of paid video streaming services is thus a distinct user experience, with materially stronger protections for children.

The Consumer Protection Rules Go Beyond the AADC Law to Restrict Legitimate, Non-Harmful Features on Paid Video Streaming Services

At the outset, MPA notes that many of the rules appear to prohibit practices based solely on a determination that the practice increases the amount of time a minor spends using an online service. This is beyond the legislature's directive. The AADC Law directs the Attorney General to identify design practices and data processing methods that lead to "compulsive use or subvert or impair user autonomy, decision making, or choice."[5] Rules based solely on a determination that a practice constitutes "engagement optimization," including any practice that increases the

---

[2] *See* Classification and Rating Administration, https://www.filmratings.com/.
[3] *See* TV Parental Guidelines, https://www.tvguidelines.org/aboutUs.html.
[4] See https://help.netflix.com/en/node/264; https://help.disneyplus.com/article/disneyplus-parental-controls; https://help.hulu.com/article/hulu-restrict-content; https://help.hbomax.com/kn-en/answer/detail/000002540; https://www.amazon.com/gp/help/customer/display.html?nodeId=GYBCCNGWAJFEUVG3; https://www.peacocktv.com/help/article/does-peacock-have-parental-controls; https://support.paramountplus.com/s/topic/0TO0y000000ADlZGAW/parental-controls?language=en_US; https://help.crunchyroll.com/hc/en-us/articles/30662259576340-How-to-set-up-Content-Restrictions.
[5] 9 V.S.A. § 2449f(b).

amount of time a minor spends on a service, are thus outside of this delegation of authority.[6] The same is true for rules that purport to restrict practices that lead to "compulsive use," where the CP Rules have effectively ignored the statutory definition requiring that such use "materially disrupts one or more major life activities of a minor," including in the Compulsive Use Rule (CU Rule) itself.[7]

Other similar departures from the statute create pervasive overbreadth. For instance, some of the CP Rules do not restrict a particular design or data practice, even though that is what the legislature directed the Attorney General to do. *See, e.g.*, General Duty Rule;[8] Monitoring & Tracking Rule.[9] The CP Rules also state that they apply where a covered business "knows or has reason to know that a user is a covered minor," and defines "reason to know" to include when a covered business is "reasonably likely to be accessed by a covered minor."[10] The AADC Law, however, imposes an actual knowledge standard.[11]

Beyond these overarching concerns, numerous restrictions in the CP Rules would impair standard features of paid video streaming services, create unnecessary friction for minor users, and contradict the AADC Law.

1. **Overbroad "Recommendation" Restrictions Impede Personalized Content-Discovery Pages for Streaming Service Catalogs**

The CP Rules contain onerous, overlapping restrictions on recommending content to minors that materially exceed the restrictions enacted in law. The AADC Law struck a balance for covered businesses that wanted to recommend media content to minors with **statutory exemptions**. Under the law, a covered business cannot use "the personal data" of a covered minor to "select, recommend, or prioritize media" for that minor, *except* if the personal data falls into an exemption—including requests to see more or less content from particular sources, requests to see certain categories of media, requests to see more or less media with "similar characteristics," and search queries.[12] The Draft Rules go much further, broadening the blanket restrictions and effectively writing out the exemptions, while expanding the types of data and recommendations that covered businesses cannot use. For example:

- **Behavioral Recommendations System Rule (BRS Rule):** While the AADC Law prohibits certain recommendations based on "personal data," ***the BRS Rule adds***

[6] *Martin v. Agency of Transp. DMV*, 819 A.2d 742, 749 (Vt. 2003) ("It is axiomatic that an administrative agency's power to promulgate regulations may extend only as far as its legislative grant of authority. . . . If an agency operates outside the bounds, or for purposes other than those, authorized by the enabling legislation, 'this Court will intervene.'").
[7] *Compare* 9 V.S.A. § 2449a(8) *with* CP Rules at 7 (a practice is deemed to lead to compulsive use where it "[i]s designed or reasonably likely to increase, . . . a covered minor's interaction with the online service.").
[8] In addition to the fact that the AADC Law does not provide the Attorney General authority to promulgate a duty of care, the articulated duty appears substantively different from the one enacted in law. This is plainly beyond the scope of what the Draft Rules should cover.
[9] In addition to these specific rules, the CP Rules include numerous rebuttable presumptions and burdens of proof, which are likewise beyond the scope of the legislative directive.
[10] CP Rules at 1.
[11] 9 V.S.A. § 2449a(12).
[12] 9 V.S.A. § 2449f(a)(4).

restrictions on "behavioral data" and "inferred preferences."[13] These types of data are not defined as subsets of personal data, and so may capture information that is not linked or reasonably linkable to an individual, or that maybe de-identified or otherwise not personal data. This could even impede using aggregated and anonymous data to make recommendations. ***The BRS Rule also creates new limits on using data to "rank, order, . . . or sequence" media***. And perhaps most notably, ***the BRS Rule omits the statutory exemptions provided for in the AADC Law – effectively writing those exemptions out of the law.***

- **Personalized Media Rule (PM Rule):** Similar to the BRS Rule, the ***PM Rule restricts the use of "behavioral data" and prohibits "rank[ing], order[ing], . . . or sequenc[ing]" media based on such data.***[14] ***Additionally, while the PM Rule incorporates elements of the statutory exemptions, it narrows them substantially.*** The exemptions in the PM Rule apply only to uses of "personal data," not "behavioral data." Additionally, because the CP Rule limits the ability to treat account settings as user requests, *see infra* at 5, the exemptions are potentially substantially narrower than contemplated by the statute.

- **Secondary Use Rule (SU Rule):** The SU Rule includes a blanket prohibition on making inferences about a covered minors' "preferences, or engagement patterns," and on using any such inferences "to influence the presentation of media," and specifically identifies recommendations as secondary uses.[15] ***This rule contains none of the statutory exemptions for recommendation systems.***

- **Data Minimization Rule (DM Rule):** The DM Rule prohibits retaining personal data of a covered minor for "prioritizing, [or] recommending . . . media . . . based on behavioral data, inferred preferences, or prior activity," as well as retaining personal data for purposes of "recommendation systems," or for "engagement optimization."[16] ***None of the statutory exemptions are accounted for in this overbroad restriction.*** The DM Rule also prohibits any use of personal data that is not "necessary to provide an online service," which purports to mirror the AADC Law—except "necessary to provide a service" is newly defined to <u>*exclude*</u> use of data to "prioritize, [or] recommend" media if it is "based on behavioral data, inferred preferences, or prior activity." That ***limitation (which appears nowhere in the AADC Law) likewise expands the restrictions on recommendations.***

These restrictions are beyond those created or contemplated by the AADC Law, and in fact directly *conflict* with the law as enacted. Together, these rules jeopardize the ability to employ even basic content recommendations, for instance to recommend a new season of a television show that the minor has previously watched, content by the same studio as something the minor has previously seen, or even content from the same genre as the minor has expressly indicated they are interested in watching.

---

[13] CP Rules at 9.
[14] CP Rules at 6.
[15] CP Rules at 5.
[16] CP Rules at 4.

Where the CP Rules conflict with the AADC Law, including where they prohibit practices expressly authorized by statute, the prohibitions are improper.[17] Furthermore, each of these rules appears to be premised on an effort not to restrict "compulsive use" or "impaired autonomy," but rather to restrict features that merely increase engagement.[18] But, as noted above, prohibitions based solely on increased engagement are beyond the permissible scope of the Draft Rules.

To address these concerns, MPA proposes that the overbroad restrictions noted above be removed, that the CP Rules be clarified to confirm that the statutorily-protected recommendation tools covered by Section 2449f(a)(4) remain exempt in each instance where the Draft Rules purport to restrict recommendations. Furthermore, the types of data covered by the Draft Rules should be limited to personal data, as contemplated by the AADC Law. Finally, restrictions based solely on the potential of increased engagement should be removed in their entirety, and only those linked to compulsive use (as defined in the statute) or impaired user autonomy should remain.

2. Jeopardizing Reliance on Account Settings, Including Those Established by Parents to Provide Age-Appropriate Content

The CP Rules would appear to limit the ability to rely on account settings when offering content to minors. The CP Rules newly define the term "express and unambiguous request" to be a "specific and contemporaneous request affirmatively initiated by a covered minor."[19] This is a critical definition, as many of the CP Rules condition a covered business' conduct on obtaining such a request. The requirement that a request be "contemporaneous" and "initiated by a covered minor" could disqualify account settings—including indications of what genre or age-rating of content should be made available to an account holder. The requirement that such a request be "initiated by a covered minor" may also disqualify settings and preferences established by the parent who sets up a child's account—which undermines the purpose of the AADC Law.

The problems that arise from the overly narrow definition of "express and unambiguous request" stem from numerous individual rules, including:

- **PM Rule:** As noted above, the statutory exemptions expressly permit certain content recommendations to minors. While the PM Rule incorporates the statutory exemptions, it requires the request be "contemporaneous" and "initiated by the covered minor," which casts doubt on the ability to rely on account settings (including settings directing that only certain age-appropriate content should be

[17] *See Lemieux v. Tri-State Lotto Comm'n*, 666 A.2d 1170, 1175 (Vt. 1995) ("We cannot enforce administrative rules if they are inconsistent with the authorizing statute.").
[18] *See* DM Rule ("Personal data of a covered minor shall not be retained for purposes of: . . . Engagement optimization."); SU Rule ("A covered business shall not: . . . Use such inference to influence . . . engagement of covered minors."); PM Rule ("prohibited uses include any use of personal data or processing that: . . . customizes media in a manner . . . reasonably likely to increase engagement"); BRS Rule (barring systems that "rely on engagement optimization").
[19] CP Rules at 2.

shown to a minor).[20]

- **DM Rule:** The DM Rule prohibits retaining or using "personal data" unless it is "necessary to provide" an online service.[21] Because the CP Rule incorporates the defined term "express and unambiguous request" into the definition of "necessary to provide," the DM Rule may restrict the collection or use of account settings insofar as such settings are not "contemporaneous" information.

- **SU Rule:** The definition of "secondary use" incorporates the term "necessary to provide," and so in turn incorporates the term "express and unambiguous request."[22] This further appears to restrict the ability to rely on account settings.[23]

User account settings on paid video streaming services provide parents with the ability to establish guardrails on the accounts accessed by their minor children, including control over what they are allowed to watch. The overly narrow definition of "express and unambiguous request" in the CP Rules threatens the ability to rely on these settings, and should be revised or removed in its entirety, to align with the statute and protect the ability to rely on account settings and other non-contemporaneous preferences.

3. Non-Productive Mandatory "Monitoring" Signals

The Monitoring and Tracking Rule (MT Rule) imposes an overbroad and ineffective signal requirement that could, in practice, be required any time a covered minor uses a covered business' service. The MT Rule requires a "continuous, real-time, visible" signal if a covered business is "[m]onitoring or tracking" a covered minor.[24] "Monitoring" is defined to include "observing" and "collecting" a minor's "activity, behavior, or interactions" with a service.[25] Under this definition, even logging which episodes of a television series a minor has watched—to provide the next one in the series when the minor next logs in, or a "watch history" feature—may constitute "monitoring" and thereby require a persistent, visible notification on the user's screen. Requiring a signal in this circumstance is so plainly overbroad it will result in label fatigue (causing users to ignore more useful labels or warnings).

Furthermore, the MT Rule is beyond the scope of what the AADC Law indicates the Draft Rules should govern. The statute directs the Attorney General to adopt rules to "prohibit[] data processing or design practices" that lead to compulsive use or impair user autonomy.[26] The MT Rule does not prohibit any data processing or design practice (nor, for that matter, does the

[20] CP Rules at 6.
[21] CP Rules at 4.
[22] CP Rules at 3.
[23] The SU Rule is also overly restrictive, and directly contradicts the AADC Law, insofar as it omits the allowance to make use of personal data where "necessary to comply with any obligation under this chapter." 9 V.S.A. § 2449f(a)(2).
[24] CP Rules at 5.
[25] CP Rules at 2.
[26] 9 V.S.A. § 2449f(b).

act of monitoring or tracking necessarily lead to compulsive use or impair user autonomy). The signal requirement is thus outside of the legislative grant of authority.[27]

4. Other Design Prohibitions Restrict Standard Paid Video Streaming Service Features and Are Outside the Scope of the AADC Law

Numerous other prohibitions contained in the CP Rules, which restrict design practices not referenced in the AADC Law, are similarly overbroad. The rules propose to wholesale prohibit features or tools even though those tools do not necessarily result in compulsive use and/or impair user autonomy. These prohibitions include:

- **Blanket Limits on "Autoplay" Features:** The CU Rule provides that a design practice that operates "without an express and unambiguous request by a covered minor directing the selection or continuation of media" *per se* leads to compulsive use.[28] In addition, the Autoplay Rule bans "automatically initiat[ing] media without action by a covered minor."[29] ***These restrictions could prohibit even moving to the second episode in a television series after the first one is finished (even if the user has requested this feature in account settings).***

- **Continuous Media Feeds Rule (CMF Rule):** The CMF Rule prohibits any "media stream[] that automatically load[s] or continuously present[s] additional media" absent some "discrete and intentional action" that is beyond "scrolling or navigation."[30] The rule is facially broader than so-called "infinite scroll" limitations and so ***may cover a home page on a paid video streaming service that permits a user to navigate through a finite number of choices***. The requirement that a user should have to make some "intentional action" beyond scrolling to view additional content is contrary to users' expectations for navigating a library of content and introduces needless friction.

- **Engagement-Based Notifications Rule (EBN Rule):** The EBN Rule prohibits notifications "designed or reasonably likely to encourage, increase, prolong, or reinitiate a covered minor's engagement with an online service," if those notifications use "personal data, behavioral data, or inferred preferences."[31] Once again, this rule conflates features that result in *any* increased use of a service with features that result in *compulsive* use. ***The EBN Rule would therefore appear to prohibit a paid video streaming service from sending a notification to a minor when a movie that the user added to a "Watch List" is newly available.*** The rule would prevent notifications even if the minor expressly requests to be notified, as there is no apparent consent exception. The EBN Rule (as well as parts (a) and (b) of the Push Notifications Rule (PN Rule), which includes an overlapping restriction) conflicts with the AADC Law's provision on push notifications—which clearly contemplates that covered businesses will send *some* notifications to covered minors.

---

[27] *See Martin*, 819 A.2d at 749.
[28] CP Rules at 7.
[29] CP Rules at 9.
[30] CP Rules at 10.
[31] CP Rules at 10-11.

Insofar as these rules apply broadly to services that increase user engagement—but do not result in "compulsive use" or "impaired autonomy"—they should be removed or modified to be within the confines of the AADC Law and the Attorney General's authority.

The Age Assurance Rules Create Tensions Without Adequate Guidance for Covered Businesses to Resolve

Separate from the design and data restrictions contained in the CP Rules, the AA Rules likewise introduce compliance challenges that merit revision before the rules go into effect. These include the following three areas of concern:

- **Clarity on Approved Age Assurance Methods:** MPA appreciates the recognition that different services present different risks. However, the framework provided by the AA Rules ultimately fails to provide sufficiently specific guidance for companies to ensure they are compliant or clear indications as to under what circumstances the Attorney General will find an age assurance method either too intrusive or insufficiently intrusive.

- **Overbroad "Linking" Prohibition:** The Linkability & System Design Rule restricts "linking" across different online services, in a way that could introduce unnecessary friction for services accessed by the same account.[32] A user that has undergone age assurance processes in connection with their account should not be required to undergo such a process again when using that account to access a different service within the same online ecosystem. At the very least, the age determination (separate from any raw data used to make the determination) should be permitted to be shared across different online services controlled by the same covered business and accessed by a user through the same account or profile.

- **Overly Cumbersome Appeals Requirements:** The Appeals Process Rule creates a novel and unduly burdensome procedure for appeals. The rule requires an independent human review of "any age-related determination."[33] While human review may be appropriate in some circumstances, the prohibition on automated reviews – even in circumstances of fraudulent requests or those where a user declines to provide any additional information – creates a substantial operational burden and should be narrowed to permit automated reviews where appropriate.

* * * *

MPA appreciates your attention to these important issues. Please feel free to reach out to me at Kathy_Banuelos@motionpictures.org, or our legislative advocate, Michelle Farnham at (802) 861-7761, with any questions concerning the above issues or the Draft Rules.

[32] AA Rules at 7-8.
[33] AA Rules at 10.

Sincerely,

Kathy Bañuelos



Senior Vice President, State Government Affairs
Motion Picture Association

Bambara, Anthony

Subject: Ad Trade Opposition to Vermont AADC Rulemaking

From: Adam Wadsworth <awadsworth@ana.net>
Sent: Friday, October 2, 2026 11:22 AM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: Ad Trade Opposition to Vermont AADC Rulemaking

Some people who received this message don't often get email from awadsworth@ana.net. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Dear Attorney General Clark:

Please find attached a letter from the following advertising trade associations in opposition to the **proposed rules implementing the Vermont Age-Appropriate Design Code Act:** the Association of National Advertisers, the American Association of Advertising Agencies, the American Advertising Federation, and the Digital Advertising Alliance. We appreciate your consideration of this letter.

If you have any questions about this letter, please feel free to reach out to Chris Oswald at coswald@ana.net.

Best Regards,

Adam Wadsworth

Adam Wadsworth
Coordinator, Law, Ethics, Govt Relations
Association of National Advertisers (ANA)
P: 202.861.2430 | C: 239.851.5300 | **ana.net** | **LinkedIn**
2020 K Street, NW, Suite 660, Washington, DC 20006
The ANA drives growth for you, your brand, our industry, and humanity. Learn how at ana.net/membership.



October 2, 2026

Charity R. Clark, Vermont Attorney General
Office of the Attorney General
State of Vermont
109 State Street
Montpelier, VT 05609

Re: Comment – Vermont Age-Appropriate Design Code Rulemaking

Dear Attorney General Clark:

On behalf of the responsible advertising industry, we provide the following comments in response to the Attorney General's proposed rules implementing the Vermont Age-Appropriate Design Code Act ("AADC").[1] We support the Vermont legislature's goal of protecting minors online. Below, we offer comments to help refine the proposed rules so that they remain clearly grounded in the scope of the AADC's rulemaking authority. Our central concern is that several provisions of the proposed rules extend beyond the areas the legislature directed the Attorney General to address via regulation, creating uncertainty and unintended potential legal vulnerability.

I. The Proposed Rules Should Be Aligned with the Scope of the AADC Rulemaking Authority

The Attorney General's rulemaking authority under 9 V.S.A. § 2449f is limited and purposeful: the legislature authorized the Attorney General to adopt rules prohibiting data processing or design practices that (1) lead to compulsive use, or (2) subvert or impair user autonomy, decision-making, or choice.[2] This is not a general grant of authority to regulate all of the design and operation of online services; it is, rather, a targeted mandate focused on two specific outcomes. Below is a non-exhaustive list of areas where we are concerned the proposed rules depart from this limited delegation of rulemaking authority.

- **Overbroad Applicability Provision.** The proposed rules apply to "the design, development, and operation of any online service, product, or feature that is used by a covered minor."[3] This formulation departs from the AADC's applicability standard in two significant respects. First, the statute applies to businesses "whose online products, services, or features are reasonably likely to be accessed by a minor," not to services that have ever been *used by* a minor, an expansion that would exceed the statute's scope.[4] The "is used" standard would bring every online service under the rules' scope if even a single minor has accessed it, leading to a result that would regulate services far beyond

[1] Vermont Age-Appropriate Design Code Rulemaking *available* here. Hereinafter, the first proposed rule is referred to as "Prohibited Data and Design Practices Rule" and the second proposed rule is referred to as "Age Assurance Privacy Rule" (collectively, "proposed rules").
[2] 9 V.S.A. § 2449f(b).
[3] Prohibited Data and Design Practices Rule, CP_Applicability (a) at 1.
[4] 9 V.S.A. § 2449a(10).

those the legislature intended to cover and lead to technical violations which will divert attention and resources from substantive work. Second, this language converts the legislature's narrow rulemaking delegation into a general-purpose design regulation with no required connection to compulsive use or impairment of autonomy. For instance, several major provisions of the proposed rules, including data minimization requirements, secondary use restrictions, and personalized media bans, are framed as general obligations applicable to all covered businesses without any showing that the regulated practice leads to compulsive use or impairs autonomy.[5] The AADC does not authorize broad design mandates separate from the two enumerated effects to trigger rulemaking.

- **Flat Ban on "Secondary Use" Is Outside the Scope of Rulemaking Authority.** The proposed rules would prohibit using personal data associated with a covered minor "for any purpose other than the purpose for which it was collected" and expressly provides that neither "disclosure to" nor "consent by" a covered minor makes secondary use permissible.[6] The proposed rules flatly prohibit profiling, recommendations, advertising, and model training, labeling these activities "secondary uses" that are barred "regardless of disclosure."[7] These prohibitions apply without any consideration whether the use leads to compulsive use or impair user autonomy—the only areas which the legislature authorized the Attorney General to regulate. The proposed rules also would conflict with the Children's Online Privacy Protection Act, which expressly permits additional data uses where verifiable parental consent has been obtained.[8]

- **Proposed Definitions Conflict with Statutorily Defined Terms.** The AADC prohibits collecting, selling, sharing, or retaining personal data that is not "necessary to provide an online service, product, or feature with which the covered minor is actively and knowingly engaged."[9] The proposed regulations' definition of "necessary to provide a service" would change the statutory standard; for example, it imposes a "strictly required" test that the legislature did not enact, and categorically excludes advertising and analytics.[10] These proposed modifications would not implement the statutory text and would exceed the limited rulemaking authority with no required connection to compulsive use or impairment of autonomy.

- **Creation of Unauthorized Categories.** The proposed rules would create an entirely new "behavioral data" category that would encompass "clicks, scrolls, dwell time, viewing history, and navigation patterns" that the AADC does not use, define, or authorize the Attorney General to create.[11] This novel data category is then subjected to the same restrictions as personal data, exceeding the statute's limited rulemaking authority by making no connection between the limits on "behavioral data" to compulsive use or impairment of autonomy.

---

[5] *See id.* CP_Data Minimization; CP_Secondary Use; CP_Personalized Media at 4-6.
[6] Prohibited Data and Design Practices Rule, CP_Secondary Use at 5.
[7] Prohibited Data and Design Practices Rule, CP_Definitions (l) at 3.
[8] 16 CFR § 312.5.
[9] 9 V.S.A. § 2449a(26)(D).
[10] Prohibited Data and Design Practices Rule, CP_Definitions (j) at 3.
[11] Prohibited Data and Design Practices Rule, CP_Definitions (b) at 2.

- **Mandatory Age Assurance.** The AADC frames age assurance permissively. The law defines "covered minor" and "known adult" to include individuals "actually known" to be certain ages or individuals who are labeled by business to be certain ages pursuant to an age assurance method in rules adopted by the Attorney General. The rulemaking directive instructs the Attorney General to identify "commercially reasonable and technically feasible methods" for age assurance, *but not to mandate their universal deployment*.[12] Yet the proposed rules require all covered businesses to "implement proportionate age assurance measures" and "determine whether a user is a covered minor," transforming the permissive framework in the statute into a universal mandate via regulation.[13]

II. Regulatory Overreach Will Lead to Significant Consequences

The proposed rules expand requirements and obligations beyond the AADC's rulemaking delegation in ways that would carry significant real-world consequences. For instance, the categorical exclusion of advertising from "necessary" uses, combined with the blanket prohibition on secondary uses, including advertising "regardless of disclosure," would fundamentally disrupt the ad-supported business models that enable consumers to access a wide range of online services at no cost.[14] The legislature did not direct the Attorney General to restructure the economics of the Internet, but rather granted narrow rulemaking on two specific effects. The proposed rules also raise serious concerns under the First Amendment and how these regulatory mandates may apply broadly to constitutionally protected speech, as the practical effect of such mandates is to deter both speakers and audiences from engaging with protected expression.

III. The Proposed Rules Impose Unwarranted Burdens

The AADC defines "minor" as any individual under 18 years of age.[15] Because the proposed rules do not fully account for the statutory standards that rulemaking should be tied to compulsive use or subversion or impairment of autonomy, decision-making, or choice, they would apply uniformly across this entire age range without any required showing that the regulated practices actually cause the effects the legislature identified. If the proposed rules were properly scoped to those two statutory effects, age-differentiated approaches might naturally follow, as practices that lead to compulsive use in younger children may not have the same effect on older teenagers. Instead, blanket prohibitions untethered from these standards treat a 17-year-old researching college options, armed services, trade school opportunities or engaging with civic discourse the same as an 8-year-old. This one-size-fits-all result is a direct consequence of the proposed rules' departure from the AADC's limited rulemaking mandate.

Moreover, the proposed rules' universal age assurance mandates, triggered by the low two-percent threshold, could impede older minors' access to information online.[16] The friction

[12] 9 V.S.A. § 2449g(b)(1).
[13] Age Assurance Privacy Rule, CP_Applicability (c)-(d) at 1.
[14] *See Americans Value Free Ad-Supported Online Services at $1,400/Year; Annual Value Jumps More Than $200 Since 2016,* Digital Advertising Alliance, *available* here.
[15] 9 V.S.A. § 2449a(19).
[16] 9 V.S.A. § 2449a(26)(B); Age Assurance Privacy Rule, CP_Applicability (c) at 1.

imposed by mandatory age-gating may deter older teens from accessing content they have every legal right to view, effectively restricting their access to constitutionally protected expression without meaningful corresponding benefit. A more graduated approach, with more restrictive measures for younger minors, would better serve the AADC's protective purposes while avoiding unnecessary burdens on older teens.

* * *

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country. These companies range from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,000 companies that power the commercial Internet, which accounted for nearly 20 percent of total U.S. gross domestic product ("GDP") in 2024.[17] By one estimate, approximately 18.2% of Vermont jobs in 2024 were related to the ad-subsidized Internet, a share projected to increase to 20.0% by 2029.[18] Our group has more than a decade's worth of hands-on experience it can bring to bear on matters related to consumer privacy and controls.

We respectfully urge the Attorney General to refine the proposed rules to ensure that each provision maintains a clear connection to the statutory effects of compulsive use or impairment of autonomy, avoids conflict with federal law, and does not expand the substantive reach of the underlying AADC through the rulemaking process. We welcome the opportunity to engage further with the Office of the Attorney General on these issues.

Thank you in advance for your consideration of this letter.

Sincerely,

Christopher Oswald
EVP for Law, Ethics & Govt. Relations
Association of National Advertisers
202-296-1883

Alison Pepper
EVP, Government Relations & Policy
American Association of Advertising Agencies,4As
202-355-4564

Anne Kierig
VP–Government Affairs
American Advertising Federation
202-898-0089

Lou Mastria
CEO
Digital Advertising Alliance
347-770-0322

CC: Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP
Matthew Stern, Venable LLP

[17] S&P Global, THE ECONOMIC IMPACT OF ADVERTISING ON THE US ECONOMY, 2024-2029 at 4 (Aug. 2025), located at https://theadcoalition.com/wp-content/uploads/2025/08/TAC_SP-Global-Final-Report_August-2025.pdf.
[18] *Id.* at 15-16.

Bambara, Anthony

Subject: Vermont AADC Rulemaking Submission - Future of Privacy Forum

From: Daniel Hales <dhales@fpf.org>
Sent: Friday, October 2, 2026 12:06 PM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: Vermont AADC Rulemaking Submission - Future of Privacy Forum

Some people who received this message don't often get email from dhales@fpf.org. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Good afternoon,

The Future of Privacy Forum is pleased to submit comments in response to the Attorney General's Office's NPRM on the Age Appropriate Design Code. Attached is a PDF document containing our official comment. We appreciate the opportunity to provide input on this important matter. If you have any questions regarding this comment and our recommendations, or would like to discuss any of these topics further, please feel free to contact me at dhales@fpf.org.

Sincerely,

Daniel Hales

--



Daniel Hales (he/him)
Policy Counsel, US Legislation
Future of Privacy Forum
(202) 220-8062 | dhales@fpf.org | fpf.org | 1350 Eye Street NW, Ste 350, Washington, DC 20005

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 *accuracy minimum* is defined as: (1) a rate of false positives for an age assurance method that is equal to or less than the following: ● 0.1% of minors ages 0 to 7; ● 1% of minors ages 8 to 13; ● 2% of minors ages 14 to 15; ● 8% of minors age 15; ● 15% of minors age 17 (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.** ● *Preliminary estimation:* If the covered social media platform can conclude with 80% confidence that an account holder is over 15 years old, 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. ● *Estimate revision:* If the covered social media platform can conclude with 90% confidence that an account holder is over 15 years old, 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.) ● *For new account users who have been on the platform for at least 25 hours in a 6-month period:* If the covered social media platform is able to conclude with an 80% confidence score (or greater) that the user is 16 years or older, the user will not be considered a child. ● *For new account users who have been on the platform for at least 50 hours in a 6-month*

		period: If the covered social media platform is able to conclude with a 90% confidence score (or greater) that the user is 16 years or older, the user will not be considered a child. ● *For Biannual Age Estimation Updates:* If the platform can conclude with a 90% confidence score (or greater) that the account holder is 16 years or older, 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

Bambara, Anthony

Subject: NECTA Comments on Proposed rules for Sections 2249f and 2449g of Act 63

From: Anna Lucey <ALucey@connectingne.com>
Sent: Friday, October 2, 2026 11:09 AM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Cc: Tim Wilkerson <TWilkerson@connectingne.com>
Subject: NECTA Comments on Proposed rules for Sections 2249f and 2449g of Act 63

Some people who received this message don't often get email from alucey@connectingne.com. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Anna P. Lucey

Executive Vice President of Legislative & External Affairs

New England Connectivity and Telecommunications Association

Phone: (781) 843-3418

Cell: (781) 917-4889



October 2, 2026

VIA ELECTRONIC MAIL
Office of the Vermont Attorney General
109 State Street
Montpelier, VT 05609
ago.rulemaking@vermont.gov

Re: NECTA Comments on proposed rules for Sections 2249f and 2449g of Act 63, An Act Relating to an Age-Appropriate Design Code

Dear Attorney General Clark,

The New England Connectivity and Telecommunications Association ("NECTA") appreciates this opportunity to comment on **proposed rules for Sections 2249f and 2449g of Act 63.** NECTA is a five-state regional trade association representing substantially all private telecommunications companies in Vermont, Connecticut, Massachusetts, New Hampshire, and Rhode Island. In Vermont, our member companies include Comcast and Charter Communications. The networks built and maintained by our companies deliver gigabit speeds to more Vermonters than any other provider. NECTA members serve 190 Vermont municipalities with broadband, video, voice, and home security and automation services. Over the past decade, our members have collectively invested over $200 million developing state-of-the-art networks in Vermont. Today, we provide high-speed broadband to 157,000 homes and businesses through approximately 9,000 miles of fiber.

NECTA Members' Services are Curated, Household-Based Services that Already Protect Minors

NECTA members' services are fundamentally different from the social media and other open, free-to-use platforms that motivated Vermont's Age-Appropriate Design Code Law (AADC). Those platforms distribute content uploaded by millions of individual users, often making it instantly available to broad audiences, including children. NECTA members, by contrast, operate paid, household-based services established and managed by an adult account holder. Its

53 State Street, Suite 525 Boston MA 02184 781.843.3418 connectingne.com

programming is professionally produced and licensed, offered within a curated and controlled environment, and supported by robust parental safeguards. For example, depending on the service, parents can block channels and titles by rating and require a personal identification number, or PIN, for purchases or mature content, and create kids' profiles that limit the catalog to age-appropriate programming. Linear and live television, in turn, is scheduled and presented by the programmer in real time and the sequence of programming on a channel is not personalized to any viewer. These services offer distinct user experiences with materially stronger protections for children and should not be regulated as open, user-generated social media platforms.

The Proposed Rules Would Disrupt Everyday Cable and Streaming Experiences Without Advancing the AADC Law's Protections for Minors

The AADC directs the Attorney General to adopt rules prohibiting data processing and design practices that lead to "compulsive use" or that subvert or impair user autonomy, decision making, or choice (the "Design Rules").[1] The Design Rules do not remain within those statutory bounds. Instead, they broadly restrict ordinary service features whenever those features may increase engagement and bear no reasonable relationship to compulsive use or impaired autonomy. That overbreadth is particularly ill-suited to paid cable and streaming services. By applying concepts developed for open-ended, algorithmically driven social media feeds to professionally curated, household-based video services, the Design Rules would restrict routine functions that help subscribers navigate programming and operate the service safely and reliably. The result would be a degraded user experience without a corresponding benefit to minors—and, in some instances, would make it harder for parents and children to locate and use age-appropriate content.

1. Overbroad "Recommendation" Restrictions Would Force Cable and Streaming Services to Present a Static, Uncurated Catalog

The AADC prohibits a covered business from using the personal data of a covered minor to "select, recommend, or prioritize media" for that minor, but expressly preserves recommendations based on a minor's requests to see more or less content from particular sources, requests for particular categories of media, requests for media with "similar characteristics," and search queries.[2] The Design Rules substantially expand this restriction and effectively write the statutory exemptions out of the law:

- **Personalized Media Ban:** The Personalized Media Ban prohibits the use of personal data or behavioral data to "select, recommend, rank, order, prioritize, or sequence media" for a covered minor, and expressly targets "For You" feeds and media ordered based on prior viewing behavior. Although the Personalized Media Ban incorporates elements of the statutory exemptions, it applies them only to "personal data" and conditions them on an "express and unambiguous request" (discussed in Section 2 below), narrowing them far beyond what the legislature enacted.

[1] 9 V.S.A. § 2449f(b).
[2] 9 V.S.A. § 2449f(a)(4).

- **Behavioral Recommendation Systems Ban:** The Behavioral Recommendations Systems Ban prohibits any system that uses personal data, behavioral data, or inferred preferences to select, recommend, or prioritize media, and omits the statutory exemptions altogether. Because "behavioral data" and "inferred preferences" are not defined as subsets of personal data, the Behavioral Recommendations Systems Ban could reach aggregated and de-identified data, calling into question even non-personalized rankings such as "Trending Now" or "Most Popular."

For subscription video services, recommendation and ordering functions are not an add-on; they are how subscribers navigate a catalog of tens of thousands of on-demand titles and hundreds of linear channels. As drafted, these rules would prohibit a "Continue Watching" row that lets a child resume the cartoon they were previously watching, a "Recommended For You" row drawn from a kids' profile's catalog of age-appropriate titles, a prompt that a new season of a previously watched series is available, and a program guide that surfaces a household's favorite channels first. The result would be a static, uncurated catalog that makes it much *harder* for minors to find age-appropriate programming and *increases* the likelihood that they will browse through content outside their interests or maturity level. None of these features leads to "compulsive use" as the statute defines it, and each is squarely within the kinds of recommendations the legislature chose to preserve in Section 2449f(a)(4).

The restrictions noted above are consolidated into a single provision that tracks Section 2449f(a)(4) and its exemptions. The consolidated rule should: (a) distinguish engagement-optimization personalization from user-directed and safety-enhancing personalization, expressly permitting recommendations that respond to stated preferences, profile settings, watchlists, ratings, genre selections, and parental controls; and (b) apply only to individualized personal data, confirming that aggregate or contextual ranking signals such as "Trending" or "Most Popular" are permitted. Alternatively, the Design Rules should expressly exempt linear, streaming, and live television programming, which is professionally curated, distributed within a controlled service environment, and fundamentally unlike the open-ended, user-generated social media feeds that lie at the core of the concerns the AADC was enacted to address.

2. The Narrow "Express and Unambiguous Request" Standard Jeopardizes Reliance on Profile Settings and Parental Controls

The Design Rules define an "express and unambiguous request" as "a specific and contemporaneous request affirmatively initiated by a covered minor." This is a critical definition as many of the Design Rules condition permissible conduct on obtaining such a request. Nothing in the AADC imposes a contemporaneity requirement or limits the relevant request to one initiated by the minor.

This definition does not reflect how subscribers communicate their choices on modern cable and streaming services. Subscribers routinely express their preferences through affirmative actions: a parent creates a kids' profile, selects a maturity level, or blocks particular channels; a teenager adds titles to a watchlist, rates programs, selects favorite genres, or enables auto-advance in the profile settings. Each of these choices is a meaningful expression of intent about how the service should operate—not an absence of choice merely because it remains in effect beyond the moment it is made. Requiring every request to be "contemporaneous" could nevertheless invalidate these persistent settings and force minors to restate the same preferences during every session or before each use of a feature. Likewise, requiring the request to be "initiated by a covered minor" could nullify choices made by the parent or guardian who established and manages the household account, including choices specifically intended to protect the minor. Those results would elevate repetitive prompts over genuine user and parental direction, undermine parental authority, and frustrate rather than advance the protective purpose of the AADC. Accordingly, the definition should be revised to remove the term "contemporaneous" and to confirm that an express and unambiguous request includes persistent user preferences, profile and account settings, watchlists and ratings, and settings or parental controls established by a parent or guardian on the minor's behalf.

3. The Data Minimization and Secondary Use Rules Would Restrict Routine Service Operations Without Any Corresponding Benefit

The AADC requires covered businesses to limit the processing of a minor's personal data to what is necessary to provide the service and expressly allows processing "necessary to comply with any obligation under this chapter."[3] The Design Rules go much further:

- **Data Minimization Standard:** The Data Minimization Standard limits collection to data "strictly required" for a feature "directly responsive to an express and unambiguous request," and redefines "necessary to provide" an online service to exclude using data to prioritize or recommend media based on behavioral data, inferred preferences, or prior activity. Taken literally, the Data Minimization Standard could restrict the background operations that make a cable or streaming service function at all—adaptive bitrate streaming, network optimization, device authentication, outage detection, diagnostics, service maintenance, and the storage of watch position needed to resume a program—none of which is "directly responsive" to a contemporaneous request.
- **Secondary Use Ban:** The Secondary Use Ban prohibits using personal data for any purpose other than the purpose for which it was collected, bans profiling and inferring behavioral traits or preferences, and provides that consent does not cure a secondary use. Thus, even where a parent or minor affirmatively opts in to a feature, the service could not use the data to provide it. The Secondary Use Ban also omits the statutory allowance for processing necessary to comply with the AADC itself.

[3] 9 V.S.A. § 2449f(a)(2).

These restrictions could, for example, call into question the use of data for essential functions such as detecting security threats and protecting networks, authenticating devices, troubleshooting subscriber streaming issues, and complying with legal obligations related to closed captioning, emergency alerts, and recordkeeping. They would also prevent a household from choosing features for their children that they believe are beneficial. The Data Minimization Standard should therefore be aligned with the well-established "support for the internal operations" exception under the Children's Online Privacy Protection Act ("COPPA") Rule.[4] The Secondary Use Ban should likewise include exceptions for secondary uses reasonably necessary to provide or maintain the service, prevent fraud, protect security, and comply with legal obligations (including obligations under the AADC), and should permit uses to which a minor or parent has affirmatively consented.

4. The Continuous Media Feeds and Autoplay Rules Mischaracterize Risk

The Draft Rules would restrict design features that are central to the cable and streaming experience and bear no resemblance to the social media practices the AADC addresses:

- **Continuous Media Feeds Ban:** The Continuous Media Feed Ban prohibits any media stream that "automatically load[s] or continuously present[s] additional media" absent a discrete and intentional action beyond scrolling or navigation. The rule is facially broader than an "infinite scroll" restriction. It could reach a streaming home page that loads additional rows of titles as a subscriber browses a finite catalog, an interactive program guide, and, most fundamentally, a linear television channel, which by its nature continuously presents programming until the viewer changes the channel or turns off the television.
- **Autoplay Ban:** The Autoplay Ban prohibits "automatically initiat[ing] media without action by a covered minor," and the Design Rules treat as per se compulsive any design practice operating without an express and unambiguous request directing the selection or continuation of media. These provisions would directly prohibit auto-advancing to the next episode of a series the minor chose to watch—even where the parent or minor enabled that setting—and could be read to reach live television that begins playing the next scheduled programming.

Browsing a professionally curated catalog is a content-discovery activity, not a content-consumption feed of endless, algorithmically selected user uploads. Likewise, sequential playback of the next episode within programming the user selected respects, rather than subverts, the user's choice, and linear and live television is scheduled by the programmer for all viewers alike. Requiring a subscriber to take some additional "intentional action" to see the next row of titles, or to resume the next episode of a children's series, introduces needless friction without addressing any risk of compulsive use.

[4] See, 16 C.F.R. §§ 312.2, 312.5(c)(7

Consequently, the Design Rules should distinguish continuous-consumption feeds from browsing and discovery interfaces, such as home pages, catalog rows, and program guides. Similarly, the Autoplay Ban should distinguish between the automatic playback of unrelated content and the sequential playback of user-selected programming and should honor autoplay settings selected by a parent or minor. Alternatively, the Design Rules should expressly exempt linear, streaming, and live programming, which presents professionally curated content within a finite, controlled environment and does not create the open-ended, algorithmically driven consumption patterns or compulsive-use risks associated with social media infinite scroll.

5. The Mandatory Monitoring and Tracking Signal Provides No Benefit

The Design Rules require a "clear, continuous, real-time, and unavoidable visual indicator" whenever a covered business monitors or tracks a covered minor (the "Monitoring Rule"). "Monitoring" is defined to include observing and collecting a minor's activity, behavior, or interactions with a service. Virtually every function of a cable or streaming service involves some collection of activity, such as logging the content being viewed, saving the minor's place in an episode, or measuring stream quality. The Monitoring Rule would therefore require a persistent visual indicator to remain superimposed on the programming throughout every viewing session, obscuring the programming, interfering with closed captions and emergency alerts, and producing label fatigue that would cause viewers to ignore more meaningful notices. The Monitoring Rule also exceeds the Attorney General's authority. The AADC directs the adoption of rules "prohibiting" data processing or design practices that lead to compulsive use or impair autonomy;[5] the Monitoring Rule does not prohibit any such practice.

Accordingly, the Monitoring Rule should be removed as it exceeds the Attorney General's statutory authority and provides no meaningful additional protection for minors. The AADC already requires covered businesses to provide a conspicuous signal when a minor's online activity or location is being monitored or tracked by another individual, thereby addressing the transparency concerns regarding such monitoring.[6] The Monitoring Rule goes substantially further by effectively requiring a persistent, real-time visual indicator during ordinary service operations, even where no heightened risk to minors is present. That requirement is not grounded in the statute and would provide little, if any, corresponding benefit to minors.

6. The Engagement-Based Notification Restrictions Would Prohibit Notifications That Subscribers Request

The Design Rules prohibit notifications "designed or reasonably likely to encourage, increase, prolong, or reinitiate a covered minor's engagement with an online service" if they use personal data, behavioral data, or inferred preferences (the "Notification Ban"). Once again, the rule

[5] 9 V.S.A. § 2449f(b).

[6] 9 V.S.A. § 2449f(a)(3).

conflates increased use of a service with compulsive use. It would appear to prohibit a notice that a program on the minor's watchlist is now available on demand, a reminder that a sports event the minor selected is about to air, or an alert that a scheduled recording is complete, even where the minor or parent affirmatively requested the notification, because the rule contains no consent exception. To account for customer consent and requests, the Notification Ban should expressly permit notifications that are responsive to an affirmative setting, a parent or guardian request, as well as service, account, security, and safety notices.

The Age Assurance Rules Impose Impractical Burdens on General-Audience, Household-Based Services

Section 2449g directs the Attorney General to adopt rules for age assurance (the "Age Assurance Rules") that prioritize user privacy and accessibility over accuracy and to consider covered businesses' size, resources, and technical capabilities; the cost and effectiveness of available methods; and their effects on user safety, utility, and experience. The Age Assurance Rules depart from those standards by imposing prescriptive requirements that favor accuracy over privacy and accessibility and do not adequately account for business capabilities, implementation costs, or the user experience. As applied to a general-audience cable and streaming service, where an adult account holder establishes service and controls access for the household, the Age Assurance Rules would require costly, redundant systems that impose friction on adult subscribers while offering little additional protection beyond existing parental controls.

1. The Rules Effectively Require Universal Age Assurance of All Users, Including Adults

The Age Assurance Rules apply when a covered business "knows or reasonably should know" that a user is a covered minor and deem a business to have such knowledge when its service is "reasonably likely to be accessed by" minors. Because almost any television or streaming service is reasonably likely to be accessed by some minors, this constructive knowledge standard would effectively require NECTA members to conduct age screening of every user, including the adult account holders who make up the overwhelming majority of its subscriber base, on every device and profile in the home. Universal age assurance is impractical for a household service. A single account may be accessed on multiple devices by several family members, and the subscriber relationship already runs to a verified adult who has agreed to service terms and payment. Requiring each viewer to undergo age assurance would impose substantial burdens on adults, require collection of additional sensitive data, and conflict with the data minimization principles the Design Rules themselves espouse. These burdens outweigh any benefit given the age screening already conducted. Therefore, the Age Assurance Rules be narrowed so that general-audience services are not required to conduct universal age assurance, and that services may rely on account-level information, including the adult account holder's status and the designation of kids' or teen profiles by the account holder, to satisfy their obligations.

2. The Least-Intrusive, Graduated Escalation, and Accuracy Requirements Create an Unresolvable Compliance Dilemma

The Age Assurance Rules require covered businesses to use the "least intrusive age assurance process," to follow a three-tier graduated escalation process when selecting methods, and to evaluate the accuracy and error rates of their methods, without defining the threshold at which a "material risk of misclassification" arises. Together, these provisions place covered businesses in an untenable position: they must choose less intrusive, and generally less accurate, methods, yet face liability if a minor is not identified. The Age Assurance Rules provide no clear indication of when the Attorney General would regard a method as too intrusive or insufficiently accurate. Absent clear guidance, companies may be pushed toward more intrusive methods to limit liability, which is contrary to the privacy interests the rules seek to protect. To ensure that companies can comply with the rules in a manner consistent with the privacy interests they are intended to protect, the Attorney General should replace the graduated escalation framework with a published list of approved age-assurance methods and establish a presumption of compliance for businesses that use an approved method. Companies using an approved method in good faith should not be liable solely on the basis of individual misclassifications, and any accuracy evaluation requirement should be tied to a defined, objective standard.

3. The Age Assurance Data Minimization and Linkability Rules Would Prevent Consistent Protections Across Services

The Age Assurance Rules impose data-minimization and linkability restrictions that, although intended to protect privacy, could undermine consistent application of age-based protections and result in duplicative data collection. Specifically, the rules would prevent covered businesses from retaining the limited information necessary to document and apply an age determination or from relying on that determination across services accessed through the same account or profile. As a result, businesses may be required to repeat the age-assurance process for the same user, potentially requiring additional collection of personal information without providing a corresponding privacy benefit.

- **Strict Data Minimization for Age Assurance Data**: The Age Assurance Rules require immediate deletion of age assurance data after an age determination, preventing a company from retaining the information needed to substantiate that determination. This requirement conflicts with the Age Assurance Rules' own documentation and oversight obligations and could leave a company unable to respond meaningfully to an appeal, parental inquiry, or enforcement inquiry by the Attorney General. Additionally, the prohibition on combining age assurance data with other personal data could prevent companies from using that information as necessary to comply with legal obligations and to apply age-related settings, protections, and experiences appropriately. Accordingly, the rules should permit retention and limited use of age assurance data where reasonably necessary to comply with law, demonstrate compliance, resolve disputes or appeals, protect security and prevent fraud, and support age-appropriate experiences.

- **Cross-Service Linkability Ban:** The Age Assurance Rules require covered businesses to minimize "linkability" across online services. That restriction does not account for integrated ecosystems in which subscribers use a single household account or profile to access multiple services and devices. If an age determination made for that account or profile could not be recognized across those services, users would be required to repeat the age-assurance process each time they access a different service through the same account. This would introduce unnecessary user friction, require duplicative processing and potentially additional collection of sensitive information, and create a risk that age-based settings and parental controls would be applied inconsistently across services. None of those outcomes advance the protection of minors or data-minimization objectives. At a minimum, the rule should expressly permit a covered business to share and rely on an age signal or age determination across services under its common control when those services are accessed through the same account or profile. Allowing reuse of the determination, without reuse or disclosure of the underlying data, would preserve privacy while enabling consistent protections and a seamless user experience.

4. The Mandatory Human-Reviewed Appeals and Fallback Mechanism Requirements Are Unduly Burdensome

The Age Assurance Rules require independent human review of any age-related determination. While human review may be appropriate in some circumstances, a categorical prohibition on automated review, including where a request is fraudulent or the user declines to provide additional information, would impose substantial operational burdens across a large subscriber base without improving outcomes. The burdens imposed by this requirement therefore substantially outweigh its benefits, and the rules should permit automated review in the first instance, with escalation to human review at the user's request. Further, the Age Assurance Rules require every age assurance method to be paired with a backup method that complies with all of the same requirements, effectively requiring businesses to build and maintain two parallel age assurance systems. The blanket fallback requirement should be removed, and a secondary age-assurance mechanism should be required only when the primary method is not reasonably accessible to a particular user, such as due to a disability or the lack of required documentation.

Thank you again for the opportunity to comment on the Proposed Regulations. We look forward to further dialogue with your office on this topic.

Sincerely,



Timothy O. Wilkerson
President

Bambara, Anthony

Subject: comments on proposed rules for Act 63, An Act Relating to an Age-Appropriate Design Code

-----Original Message-----
From: Blake C. Stacey <bstacey@mit.edu>
Sent: Friday, October 2, 2026 12:07 PM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: comments on proposed rules for Act 63, An Act Relating to an Age-Appropriate Design Code

[Some people who received this message don't often get email from bstacey@mit.edu. Learn why this is important at https://aka.ms/LearnAboutSenderIdentification]

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Good afternoon. Please find attached my comments on the proposed rules for Act 63, the Age-Appropriate Design Code.

Regards,

Blake C. Stacey

Comment on Proposed Rules for Social-Media Legislation

To Whom It May Concern:

As an operator of an independent, nonprofit social-media forum that focuses on critiquing the excesses and evils of the tech industry, I have grave concerns regarding the "Age-Appropriate Design Code" and the proposed rules pursuant to it. I have been trying to steer people away from "Big Tech" since long before that became politically fashionable. It would be counterproductive indeed to treat hobbyists, volunteers and small-scale entrepreneurs the same as one treats Instagram and TikTok: penalizing the people who are not the problem, and impeding our efforts to build alternatives to "Big Tech" that are better for young and old alike.

The Code, and the proposed rules built atop it, are fundamentally trying to regulate all communication platforms without regard to their size, amount and sources of income, and purpose. The proposed legislation attempts to penalize an entire communications medium because of the bad behavior of two or three companies. In so doing, it strangles the possibilities for a better Internet, and it harms those it is meant to protect.

I. HOW THE CODE WILL AID BIG TECH'S CONSOLIDATION OF THE INTERNET

The Code's definition of "social media platform" is quite overbroad. It is a definition one might write while trying to describe in legalese what Facebook and TikTok are, but it encompasses far more than that. Any website or online service that provides user-generated content is at risk of being implicated. Consider Wikipedia, for example. It is a platform where users "create or post content that is viewable by other users [. . .] and that presents the user with content generated by other users." It gives people the opportunity to "construct a public or semipublic profile for the purposes of signing into and using" it. It even allows a user to "populate a public list of other users with whom the user shares a social connection" (not in as automated a way as other platforms do, but the capability is there: any editor can list other editors with whom they are socially connected on their User page, and the collaborative groups of volunteers known as "WikiProjects" maintain membership lists that surely meet a plain reading of the law). Because of the "or" at the end of (27)(A)(ii), only one of these points needs to be met, and Wikipedia meets all three. The only thing that might exempt Wikipedia from being deemed a "social media platform" is the vague "primarily intended" in (27)(A); if *Wikipedia* is at risk of being regulated by the Code, then the Code was not drafted with care.[1]

One might say, "Well, Wikipedia is not *primarily* intended for social interactions among its editors, even though those are necessary for the project to function. The primary purpose is to provide an encyclopedia for everyone to read." But plenty of educational resources will lie closer to or over that line of primary intent. Education is, after all, a social activity. Consider Scirate, a nonprofit website where scientists and mathematicians bookmark and

[1] It would be, incidentally, impossible on a technical level for Wikipedia to implement the restriction that adults cannot provide feedback on "a covered minor's media". Nor does basic common sense provide a reason why a 17-year-old should be impeded from discussing an encyclopedia article.

comment upon technical publications that have yet to be formally peer reviewed. Or, consider Stack Exchange, a network of user-driven Q&A websites on many topics that began with computer programming and has since expanded to include subjects across the sciences and the arts. Asking questions and receiving answers is a social interaction, without doubt—and it does not always happen under the direction of an official educational institution.

The broad scope of the Code means that any regulations implementing it must be crafted with superlative caution. The section of the Code that directs the Attorney General to formulate rules for its implementation requires the Attorney General to consider "the size, financial resources, and technical capabilities" of covered entities, as well as "the impact of age assurance methods on users' safety, utility, and experience". Hobbyist and volunteer-operated sites simply *do not have the "financial resources"* to cope with demands for age assurance. The impact upon the users' experience is that the experience will vanish because the site can no longer operate. The tighter the regulation, the more it benefits the rich: The platforms that have the resources to comply with a strict age-gating regime are exactly those that we all, quite justifiably, dislike.

Furthermore, any age-assurance tools beyond a neutral screen (like clicking a checkbox to aver that one is over 18) are administered by the online equivalent of the Flock camera people. Forcing small platforms to hire their services isn't just a drain on those platforms' limited resources; it's outright immoral. The "privacy protections for age assurance data" won't be worth the paper they're printed on, because the age-testing industry does not have the technical competence to keep our data safe. This is not a theoretical concern: Last October, hackers broke into the service that the Discord platform used for age verification and stole the government-issued IDs of 70,000 people.[2] The Code was intended to protect minors, but instead it puts all citizens of Vermont at risk for identity theft.[3] Now that we are at the rulemaking stage, the best course of action is to trust the age-testing industry as little as possible.

The "SAFE for Kids Act" implementation rules recently promulgated by the New York Attorney General[4] represent a level of care that Vermont should at the very least meet, if not exceed. (See in particular their rules' exemptions based on platform size.) The rulemaking process should also consider the National Institute of Standards and Technology's evaluation of age-estimation technology,[5] which finds its performance to be, in a word, dreadful. Currently, the best true positive rate that NIST could find for the 13–16 range (i.e., correctly identifying those aged 13 to 16 as such) is only 72%. That's a "what are we even doing here?" success rate.[6] Australia's evaluation of age-estimation technology, in the context of their attempt to ban young people from social media altogether, found the performance in the 15–21 age range to be frankly dismal.[7] This is not an industry whose

[2] A. Belanger, "Discord faces backlash over age checks after data breach exposed 70,000 IDs," *Ars Technica,* 9 February 2026.

[3] Rep. Alexandria Ocasio-Cortez recently put the issue in appropriately stark terms: "Republicans are using kids as a smokescreen for what Big Tech lobbyists want: a national surveillance program to harvest our data with zero protections for people and their privacy." `@ocasio-cortez.house.gov` on Bluesky, 5 March 2026.

[4] `https://ag.ny.gov/safe-for-kids-act-final-rule`

[5] `https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8525.pdf`

[6] `https://bsky.app/profile/rahaeli.bsky.social/post/3mu36e5uk722g`

[7] `https://bsky.app/profile/daphnek.bsky.social/post/3mu3dwop6ms2r`

products should be pushed onto the public.

II. THE DISLIKE OF LIKE COUNTS

It is illustrative to zoom into one part of the proposed rules for Section 2249f to understand the problems involved.

The proposed rules really don't like "likes", deeming them horrible and no good and very bad for essentially no reason. Bluesky has the "popularity indicator" of like counts; Bluesky's user base has shrunk by half in two years.[8] How "addictive" can they be?

Answering machines told you how many unheard messages you had. Any email program will tell you how many unread items of correspondence you have. Wikipedia tells editors how many times they've been "thanked" by others clicking a thank-for-edit link. How are any of those different in principle from a tally of "likes"?

Clicking a heart or a star on someone's post is *sending them a message.* It's an act of *speech,* more abbreviated than saying "Nice post" but speech nonetheless. Would it be youth-hostile engagement-farming to provide a count of how many times people have replied with "nice post"? Moreover, like counts have been explicitly recognized as speech by a federal court: the Ninth Circuit found that "the regulation of like counts" is "content based", and that a law regulating how they are conveyed to users is subject to strict scrutiny.[9] In short, the proposed rules don't just have a common-sense problem, they have a Constitutional problem. And because the Code states that nothing in it "may be construed to infringe on the existing rights and freedoms of covered minors", the proposed rules are in contradiction with the Code itself.

A particular implementation of an engagement-based feed that *uses* like counts in a ruthlessly capitalist way could be harmful to some fraction of users, young or old. That doesn't make like counts *themselves* bad. In essence, the proposed rules look at gambling in casinos and declare that young people should not have access to dice.

Similarly, the proposed rules for Section 2449f prohibit "algorithmic or personalized media feeds, including 'For You' feeds". Bluesky offers such a feed as an option: the "Discover" feed, which is presented in a separate tab from the chronological "Following" feed. As noted above, Bluesky's active user base has been shrinking. If one accepts the rhetoric that algorithmic media feeds are engines of addiction, this is like watching people try cocaine and decide, en masse, "Eh, we have better things to do." Perhaps their algorithmic media feed is not so addictive after all.

This idea, that we can call a website "addictive" because of the mere presence of a feature and not how that feature is implemented or the effects a specific implementation is proven to have, is a bad mental framework to trap oneself within. It leads to overbroad restrictions and confusing exemptions, rather than a regulation that might make sense and be truly helpful. I encourage those involved in the rulemaking process to reevaluate the proposed rules' notion of "addictive" or "gamified" features with this in mind.

---

[8] Sarah Perez, "Bluesky's active user base is shrinking as its focus expands beyond the app," *TechCrunch* (August 11, 2026).

[9] *NetChoice, LLC, v. Bonta* 152 F.4th 1002 (9th Cir 2025) at 22–23.

III. INCONSISTENCY AND LACK OF CLARITY

The proposed rules for Section 2449f, under "Personalized Media", say that personal data may be used if limited to "Media sharing similar characteristics to media affirmatively selected or viewed by the covered minor." This is sensible. Publishers have been doing this for generations: If I buy a Nancy Drew book, no one objects to the list of other Nancy Drew books in the back pages. However, practically in the next breath, the proposed rules prohibit "Media ranked or ordered based on prior viewing behavior or interaction history". Bullet point (d) allows a platform to recommend more Nancy Drew to a minor who has just read Nancy Drew; bullet point (e) forbids it.

This is symptomatic of a lack of clarity in the proposal's drafting. I don't like Meta; I want young people to prosper. Carelessness is not the way to turn the Internet from a hazard into a benefit. And recall *Connally v. General Constr. Co.,* 269 U. S. 385, 391 (1926): "[A] statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application, violates the first essential of due process of law". Likewise, per *FCC v. Fox Television Stations, Inc.,* 567 U.S. 239 (2011): "Even when speech is not at issue, the void for vagueness doctrine addresses at least two connected but discrete due process concerns: first, that regulated parties should know what is required of them so they may act accordingly; second, precision and guidance are necessary so that those enforcing the law do not act in an arbitrary or discriminatory way. [...] When speech is involved, rigorous adherence to those requirements is necessary to ensure that ambiguity does not chill protected speech."

IV. CONCLUSION AND ALTERNATIVES

Recent research suggests that among young people, *moderate* social-media use is associated with better mental health than either heavy use or no use at all.[10] Correlation is not causation; heavy social-media use can be a consequence of poor mental health (e.g., seeking distraction) rather than a cause. The world has gotten worse for teens in many ways, from the vanishing of "third spaces" to the failure of institutions to care about providing a livable future, and pointing the finger at social media alone is burying one's head in the sand.[11] The social and psychological factors at work are interrelated, complicated, and difficult to study:

> Despite a wealth of research on this topic, the evidence base is currently limited in several important respects. These include primarily cross-sectional work that does not warrant causal conclusions; use of small and homogeneous samples; failure to control for confounding factors (e.g., gender); and, in the case of social media research, a predominant focus on total time spent as opposed to *how* that time is used. Finally, with a handful of exceptions, research to date has also not distinguished between-person (i.e., stable differences between individuals) from within-person (i.e., situational changes within individuals) effects. This is

[10] B. Singh et al., "Social Media Use and Well-Being Across Adolescent Development," *JAMA Pediatrics* 180 (2026), 288–97.

[11] J. Severs, "Is Jonathan Haidt right about smartphones?" *Times Educational Supplement,* 3 September 2025.

> critical because failure to do so can lead to erroneous conclusions regarding the presence, predominance, and sign of causal influences.[12]

This is not a good area in which to make blunt legal interventions. Complicated problems call for careful, flexible solutions.

I do not want to downplay the seriousness of young persons' use of social media. I have grave objections to the ways in which all of the largest social-media corporations behave, and I personally avoid all interactions with commercial social media to the fullest extent possible. I have opposed "Big Tech" for years, and I am writing out of concern that misguided attempts to regulate them will in fact entrench them. *It will be a disaster for young people if the only Internet platforms that can afford to exist are owned by billionaires.* I wish to underline that, to address the issue, we must first diagnose it properly, and then we must go about solving it in a targeted and principled way. For example, talk of "social-media addiction" is well nigh ubiquitous, yet research suggests that portraying bad social-media habits as "addiction" makes those habits harder to break.[13] No one benefits when we boil our problems all down to "dopamine".[14]

It is difficult not to mourn the missed opportunity that the Code represents. Multiple aligned pushes in the same direction could have been more effective than a single blunderbuss of an intervention. We could have put a tax on targeted advertising. We could have passed a strong privacy law that protects people of all ages, short-circuiting the toxic business models of giant corporations without "destroying the village in order to save it" by forcing platforms to gather data before deciding what amount of privacy they can offer. We could have followed a "youth center" model of reform, where we address the harms of the worst social-media platforms by giving teens better things to do on their phones. (Any minute spent playing a *Carmen Sandiego* game is a minute not spent on Instagram.) We could have encourage independent and nonprofit social media by directing young people to platforms like Dreamwidth, Bluesky and Mastodon, platforms that aren't out to exploit them. We could have educate parents about the safety features that already exist yet are under-utilized. We could have passed a law that required any smartphone vendor to ask if the device will be used by a minor, and if so, to offer to enable the parental-control measures on the device and its apps that have already been implemented. We could have done so many things. Instead, we have a "we really don't like TikTok" law that will do more harm than good, unless the rulemaking process is executed with extraordinary care and diligence.

Yours,
Blake C. Stacey, PhD
Co-moderator, TechTakes
Boston, MA
bstacey@mit.edu

---

[12] Q. Cheng et al., "How do social media use, gaming frequency, and internalizing symptoms predict each other over time in early-to-middle adolescence?" *Journal of Public Health* 48 (2026), 59–69.

[13] I. A. Anderson and W. Wood, "Overestimates of social media addiction are common but costly", *Scientific Reports* 15 (2025), 39388. https://www.nature.com/articles/s41598-025-27053-2.

[14] Nothing in brain science is as simple as a "pleasure chemical". As the neuropsychologist Vaughan Bell observed, "Traumatised war veterans, for example, show nucleus accumbens dopamine surges when they are reminded of the sounds of battle, something they find deeply aversive." See https://www.theguardian.com/science/2013/feb/03/dopamine-the-unsexy-truth.

Bambara, Anthony

Subject: Internet Works Vermont AADC Comments

From: Nicholas Krebs <nicholas@theinternet.works>
Sent: Friday, October 2, 2026 12:05 PM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Cc: Peter Chandler <peter@theinternet.works>
Subject: Internet Works Vermont AADC Comments

Some people who received this message don't often get email from nicholas@theinternet.works. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Internet Works respectfully submits the attached comments in response to the Vermont Attorney General's proposed rules implementing the *Vermont Age-Appropriate Design Code Act*, Prohibited Data and Design Practices (9 V.S.A. § 2449f) and Age Assurance Privacy (9 V.S.A. § 2449g).

Internet Works is a trade association of 34 diverse members working together to right-size technology policy, especially for Middle Tech companies.

Thank you,
Nicholas Krebs

October 2, 2026

Office of the Attorney General
109 State Street
Montpelier, VT 05609

Re: Age-Appropriate Design Code Rulemaking — Prohibited Data and Design Practices (9 V.S.A. § 2449f) and Age Assurance Privacy (9 V.S.A. § 2449g)

Dear Attorney General Clark:

Internet Works ("IW") is a trade association of 34 diverse members working together to right-size technology policy, especially for Middle Tech companies, which can best be described as small and medium-sized companies that occupy the competitive middle layer between startups and "Big Tech." While established businesses, Internet Works members are still significantly smaller and less resourced than the biggest players in the industry. Our members operate the apps, games, marketplaces, and online services that Vermonters use every day.

We appreciate the opportunity to comment on the draft rules implementing Vermont's *Age-Appropriate Design Code Act*. These rules reflect careful drafting and provide clear examples that will help guide compliance for Middle Tech companies. To strengthen the draft rules, IW recommends the following changes, with suggested new language in bold and deletions in red strikethrough.

1. Align the Conspicuous Signal and Monitoring Provisions with Section 2449f(a)(3)

The Act, specifically 9 V.S.A. § 2449f(a)(3), requires a conspicuous signal only when a covered business "permit[s] any individual, including a parent or guardian," to monitor a covered minor's online activity or track the minor's location. That signal is a cue to tell the minor an individual is monitoring them. It is not a data-processing disclosure.

Vermont's draft rule flips the Act's intent. It requires a signal for monitoring or tracking "by a covered business." Every state that has adopted an age-appropriate design code with a signal requirement for monitoring a minor's online activity ties that signal to monitoring by an individual, not to a business's data processing.

Also, the draft rule's broad definition of "monitoring" could capture a video game player's inputs, session time, or game progress. The draft rule would require an unavoidable on-screen indicator for as long as a covered minor plays a game. A permanent signal would degrade the games Vermonters enjoy. It would also invert the

General Assembly's intent, which was to require a signal when a parent or another individual is monitoring or tracking a minor.

- Amend the definition of "Conspicuous signal" to read: "Conspicuous signal" means a clear~~, continuous, real-time,~~ and **obvious** ~~unavoidable~~ visual indicator, displayed in a covered minor's primary interface **at the beginning of each session during which** ~~for the duration of any~~ monitoring or tracking activity **occurs**, that is readily noticeable and understandable to a covered minor and does not require additional action, navigation, or interpretation to identify that such monitoring or tracking is occurring.

- Amend Monitoring and Tracking (a) to read: Monitoring or tracking of a covered minor by ~~a covered business~~ **any individual permitted to do so by a covered business, including a parent or guardian,** requires a conspicuous signal.

- Amend Monitoring and Tracking (b) to read: A conspicuous signal must be ~~continuous, real-time,~~ visible~~,~~ and understandable to a covered minor.

- Strike Monitoring and Tracking (d)(1) (~~Appears only at initial use and does not persist during monitoring~~) and strike "~~intermittent,~~" from (d)(5).

2. Preserve the Gaming Experience While Prohibiting Data-Driven Rewards

The Reinforcement Mechanisms section prohibits "variable or intermittent rewards," and the examples include "points" and "gamified incentives." Applied to interactive entertainment, that language describes the structure of almost every video game that uses scores, levels, badges, achievements, and game progression. The design-feature definitions in the Senate's *Kids Online Safety Act* and the House's *KIDS Act*, both pending in Congress, restrict rewards and badges only when they are based on a minor's frequency of use or time spent. The draft rule is broader than both bills.

To address this, IW proposes subsection (c) using language from the rule's own Illustrative Applications section. This approach protects rewards that reflect or respond to a user's gameplay, while still prohibiting engagement-extending rewards.

- Amend the illustrative examples in (b) to read:
    1. Likes;
    2. **Badges or other visual award symbols based on frequency of use or time spent** ~~badges, or points~~;
    3. Intermittent feedback systems; or
    4. Gamified incentives.

- Add subsection (c): **This section shall not prohibit variable or intermittent rewards that reflect or respond to a covered minor's gameplay in an online service, product, or feature whose primary purpose is interactive entertainment, unless such rewards are timed or triggered based on a covered minor's prior activity, behavioral patterns, or inferred preferences to extend engagement or encourage re-engagement.**

- Define "intermittent feedback systems" or strike the term.

3. Adopt a Flexible, Privacy-Preserving Age Assurance Framework

IW supports systems to more accurately determine the age of users online, so platforms can comply with children's privacy laws and tailor age-appropriate experiences. We support age assurance approaches that are interoperable across states, minimize data collection, and create flexible compliance mechanisms that work.

After reviewing the draft rule, IW asks that one element be struck entirely: the term "highly intrusive age assurance," and the intrusiveness framework built upon it. No state or international regime defines "highly intrusive age assurance." New York's *SAFE for Kids Act* rules are method-neutral and instead test for accuracy. The United Kingdom's online safety regulator, Ofcom, lists acceptable methods and assesses whether age assurance is "highly effective." ISO/IEC 27566, another international standard, takes a similar approach. Every one of these frameworks grades methods by how well they work, not by an intrusiveness test.

A Vermont-only intrusiveness test would restrict commercially reasonable age assurance methods that are accepted elsewhere. It also goes against the Act's direction that the rules consider the diverse sizes, resources, and capabilities of covered businesses. IW recommends removing the intrusiveness test and preserving flexibility in acceptable age assurance methods.

Conclusion

Internet Works appreciates your consideration of our association's comments. The recommendations offered above would provide Middle Tech companies a clearer path to compliance while also advancing our shared goal of increasing trust and safety online.

Respectfully submitted,



Peter Chandler
Executive Director, Internet Works

Bambara, Anthony

From: Jameson, Sarah
Sent: Friday, October 2, 2026 12:56 PM
To: Bambara, Anthony
Subject: FW: Age-Appropriate Design Code Comment Letter
Attachments: Vermont AADC Comment Letter.pdf

From: Alex Oberg <alex@helix.id>
Sent: Thursday, October 1, 2026 4:27 PM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: Age-Appropriate Design Code Comment Letter

Some people who received this message don't often get email from alex@helix.id. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

To whom it may concern,

Please find attached our comments to your proposed age-appropriate design code. Thank you in advance for your consideration.

Best,

Alex

H3LIX AI LTD
1301 N Broadway
Los Angeles, CA 90012
alex@helix.id

Vermont Office of Attorney General
109 State Street
Montpelier, VT 05609-1001
ago.rulemaking@vermont.gov

VIA Electronic Submission

Re: Vermont Age-Appropriate Design Code Rulemaking

Dear Attorney General Clark,

This letter provides the comments of H3LIX AI LTD ("Helix") in regards to the Proposed Rules for the Age-Appropriate Design Code Sections 2449g of Act 63.

Helix applauds the Attorney General's proposed rules, especially drafting them to provide clarity and flexibility of the evolving landscape of age assurance technologies. We would like to propose three changes to the proposed language.

(1) Within the age assurance definition, we'd like to propose explicitly including ISO 275661 standards. Certification methods such as the Age Check Certification Scheme (ACCS) and International Standards Organization/International Electrotechnical Commission(ISO/IEC) standards meet recognized certification schemes or standards and have scientific support and justification for their efficacy.

Additionally, "*estimation of age based on device signals, account information or usage patterns*," is not an accurate age assurance method as this just confirms the device owner is of age, but not the user. For example, many families share computers and tech devices, particularly in less affluent households. This method would allow children to bypass all age-based controls because the device is registered to a parent. Proving who owns the device itself is very different from who uses the device and therefore the rules should highlight how to protect minors further.

Age assurance should verify a human, not a proxy. Methods like biometrics don't verify a device, phone number, image or document; they actually link online activity to a living person.

(2) Within the *Frequency and Reassessment* section of the proposed rules, it is stated the business shall not require repeated or continuous age assurance that would create additional burden. This prioritizes convenience more than safety. We'd strongly recommend removing this section as one-time verification is not an effective method. Continuous authentication ensures that the person using the platform is the same as the one that signed up. There are numerous instances reported of users gaining access to "aged" accounts well after account establishment. We would stress the importance of age-assurance controls through multiple channels as a way to combat this.

(3) For the *Graduated Escalation* section, we would recommend adding in the use of biometrics like passive voice signals from existing interactions as these methods would not require "additional personal data collection" and therefore would qualify as low-intrusion age assurance.

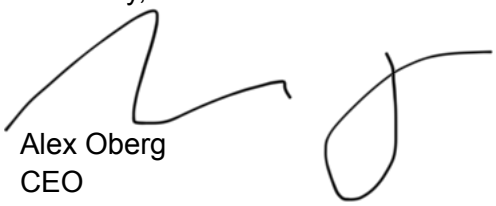
We would encourage your office to review the above proposed changes. As research shows, age estimation and assurance methods have some known issues and providing the most comprehensive rulemaking will allow Vermont to best protect minors within the state. The ***Knight Georgetown Institute Age Assurance Online: A Technical Assessment Report*** points out the following:

- Self-declaration relies on user honesty so circumvention is easy.
- Commercial and government records such as banking records, mobile network operator status and credit cards. These systems that rely on commercial transactions may be inaccessible to users with limited commercial records (i.e. those that do not hold a bank account or credit card). There are also issues with MNO-based verification as the mobile number could be tied to someone else in the family, especially with family cell phone accounts. With commercial and government records searches, providing personal information is easy to circumvent and reported false reject rates are in excess of 10%.
- Government-ID-based systems are accurate but not always available, especially for minors without government ID.
- Facial age estimation is highly available but inaccurate near the age threshold and systems based on selfies or live video may be inaccessible to users without a camera.
- Behavioral signals are less suitable for primary age assurance since they cannot determine a user's age on first contact.

Biometrics like voice can work on every device and is an effective and accurate measure for age assurance as validated by Helix's participation in ACCS's independent audit of "highly effective" methods and the ISO 27566 standard.

Thank you for your efforts on the proposed rules to make Vermont a leader in protecting minors online. We are happy to meet with the Attorney General's Office on the issues identified above or age-assurance technology more generally. Please let us know if you have any further questions in response to our suggested edits.

Sincerely,



Alex Oberg
CEO
Helix

Bambara, Anthony

From: Jameson, Sarah
Sent: Friday, October 2, 2026 12:55 PM
To: Bambara, Anthony
Subject: FW: State Privacy and Security Coalition Comments on Proposed Rules 26P027 and 26P028
Attachments: SPSC - VT AADC Rulemaking (Rule 26P027) - Comments 10.02.2026.pdf; SPSC - VT AADC Rulemaking (Rule 26P028) - Comments 10.02.2026.pdf

---

From: Willy Martinez <willy.martinez@marinerstrategies.com>
Sent: Friday, October 2, 2026 10:22 AM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Cc: Andrew Kingman <andrew.kingman@marinerstrategies.com>
Subject: State Privacy and Security Coalition Comments on Proposed Rules 26P027 and 26P028

Some people who received this message don't often get email from willy.martinez@marinerstrategies.com. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Good Morning,

On behalf of the State Privacy & Security Coalition, please find attached our comments on Proposed Rule 26P027, concerning Prohibited Data and Design Practices, and Proposed Rule 26P028, concerning Age Assurance Privacy, under Vermont's Age-Appropriate Design Code.

Please do not hesitate to reach out with any questions or if we can provide any additional information.

With our best,

Willy & Andy

--

Willy Chanes Martinez (He/Him/His)
FIP, AIGP, CIPP/US, CIPP/E, CIPM, CIPT
Associate
201.757.0115
www.marinerstrategies.com
Co-Host of ***The Spyglass*** Podcast – Listen Here!

ESTD 2022
MARINER STRATEGIES

STATE PRIVACY & SECURITY COALITION

October 2, 2026

The Honorable Charity R. Clark
Office of the Vermont Attorney General
109 State Street
Montpelier, VT 05609

RE: Proposed Rule 26P027 - Vermont Age-Appropriate Design Code

Dear Attorney General Clark:

The State Privacy & Security Coalition (SPSC) is a multi-sector coalition representing over 30 companies and seven trade associations across the retail, technology, telecommunications, healthcare, automotive, and payment card sectors. We appreciate the opportunity to comment on Proposed Rule 26P027 (Prohibited Data and Design Practices) and the Attorney General's efforts to obtain stakeholder input before the rules take effect.

SPSC supports meaningful protections for minors and the goals underlying Act 63. At the same time, the final Rules must remain grounded in the framework enacted by the Legislature and provide standards that businesses can reasonably understand and implement. Several proposed provisions extend beyond Act 63, narrow statutory exceptions, or could restrict practices that serve legitimate educational, safety, accessibility, functional, and user-directed purposes.

The implementation timeline is also a significant concern. The Proposed Rules contemplate substantial changes to existing products, data-processing practices, and technical systems, including requirements concerning monitoring and tracking, personalized media and recommendation systems, age assurance, data minimization, and third-party practices. Businesses will need time after the Rules are finalized to determine which products and features are affected, modify technical systems and product functionality, coordinate with vendors and service providers, update compliance processes, and test those changes before deployment. These steps cannot reasonably be completed until businesses know the standards ultimately adopted by the Attorney General. With the Proposed Rules currently providing for a January 1, 2027 effective date, the final Rules should provide businesses at least 12 months from publication of the finalized Rules to come into compliance with the new requirements.

Our comments focus on aligning the Rules with the Attorney General's statutory authority and the specific standards established by Act 63. In particular, the Rules should preserve the distinctions and exceptions adopted by the Legislature and avoid categorically prohibiting practices without the required connection to compulsive use or impairment of autonomy, decision making, or choice. The final Rules should also provide sufficient flexibility for different services and technologies and operate consistently with Vermont's existing privacy laws.

I. THE RULE EXCEEDS ACT 63'S DELEGATION OF RULEMAKING AUTHORITY AND EXPANDS THE STATUTE'S SCOPE

Section 2449f(b) authorizes the Attorney General to adopt rules prohibiting data-processing or design practices that "lead to compulsive use or subvert or impair user autonomy, decision making, or choice." The Rule is framed more broadly, however, by applying to the general "design, development, and operation" of services used by covered minors. *General Duty* likewise creates an obligation not to create a reasonably foreseeable heightened risk of harm. Both provisions appear to draw on § 2449c, which establishes a minimum duty of care but does not provide an independent delegation of rulemaking authority. Its scope should therefore remain tied to the specific practices and harms identified in § 2449f(b).

The Rule also expands when a user is treated as a "covered minor." Section 2449a(12) defines a covered minor as "a consumer who a covered business actually knows is a minor or labels as a minor pursuant to age assurance methods in rules adopted by the Attorney General." The definition of "known adult" likewise uses actual knowledge. By contrast, the Rule applies when a business "knows or has reason to know" that a user is a minor and deems that standard satisfied whenever a service is reasonably likely to be accessed by minors or the business "collects, processes, or infers" information indicating age. Those situations do not necessarily establish actual knowledge that a particular user is a minor. Covered-minor status should not extend beyond § 2449a(12), turning on actual knowledge or a label applied through an age-assurance method adopted under § 2449g(b), rather than a constructive-knowledge standard.

An inference-based standard could discourage businesses from voluntarily using age-related signals to provide additional protections. If using those signals to identify a user as potentially underage triggers additional legal obligations, businesses may have an incentive not to make the inference at all, even when doing so would allow them to reduce data collection or apply safer settings. The final text should clarify that protective age inferences and service-level audience indicators do not, standing alone, establish that a particular user is a covered minor. For example, prompting a user to confirm age, using conservative defaults, limiting certain features, or reducing data collection based on age-likelihood signals should not be treated as "actual knowledge" of that user's age absent a § 2449g(b) age-assurance label.

Finally, the rules assume platforms have a one-to-one user to service relationship, wherein every device is accessed by a single account, connected to only one user. This may be the case for a variety of online services, but many others utilize account architectures that allow multiple users to access a single account, across a variety of devices. The current proposed requirements are unworkable under such structures.

II. THE PROPOSED DEFINITIONS ALTER THE SCOPE AND MEANING OF ACT 63'S REQUIREMENTS

Several proposed definitions create uncertainty about what the Rule would prohibit in practice. Some introduce concepts not found in Act 63; others narrow statutory exceptions or could capture routine uses that support safety, accessibility, education, and age-appropriate experiences. The definitions should be revised so businesses can understand clearly what conduct is prohibited and what remains permitted under the statute.

- ***Behavioral Data***: The enabling statute regulates the "personal data" of a covered minor. Section 2449a(21) defines that term to cover information linked or reasonably linkable to an individual or device, but the statute does not define "behavioral data." The proposed definition could therefore sweep in clicks, scrolls, dwell time, and other signals even when they are aggregated, de-identified, or otherwise not linked or reasonably linkable to a covered minor. That expansion could restrict analytics used to improve safety, accessibility, and service quality. The definition should be deleted. If it is retained, "behavioral data" should be limited to information that qualifies as personal data under § 2449a(21), with aggregate and de-identified data expressly excluded.

- ***Heightened Risk of Harm***: As noted above, § 2449f(b) authorizes rules addressing practices that "lead to" certain prohibited practices, while § 2449a(8) defines "compulsive use" to require material disruption of a minor's major life activities. *See* 9 V.S.A. § 2449a(8). The proposed definition instead turns on a "reasonably foreseeable risk of compulsive use, impairment of autonomy" or "loss of user control over engagement." The latter concept is not enumerated in the statute and using it to trigger additional duties would expand the Rule beyond the Legislature's authorization. Accordingly, the operative definition should track the statutory language: practices that "lead to compulsive use or subvert or impair user autonomy, decision making, or choice" under § 2449f(b).

- ***Necessary to Provide a Service***: Section 2449f(a)(1) applies when personal data is not necessary to provide an "online service, product, or feature" with which a minor is actively and knowingly engaged. *See* 9 V.S.A. § 2449f(a)(1). The proposed definition narrows that standard to what is "strictly required" for a "specific feature" and adds a requirement that the function cannot reasonably be achieved through less data-intensive means. Neither limitation appears in the statute. The definition also excludes recommendations, analytics, and model training, even though § 2449f(a)(4)(A)(iii) expressly allows recommendations that show a minor media like what the minor is already viewing. The statute thus recognizes that recommendations can be part of the service.

  Accordingly, the definition should be revised as follows: "Necessary to provide a service" means "the collection, use, or processing of personal data that is reasonably necessary

to provide the online service, product, or feature with which the covered minor is actively and knowingly engaged, including processing to maintain, secure, protect, debug, improve, and ensure the integrity, safety, accessibility, and quality of that service, product, or feature."

- ***Inferred Preferences***: Section 2449f(a)(4)(A)(iii) permits a covered business to recommend "more or less media with similar characteristics as the media [the covered minor is] currently viewing." Making that recommendation necessarily requires an inference, meaning that the business must identify characteristics of the media and determine what other content to share. The definition, however, reaches any preference, interest, or affinity predicted, derived, or estimated from a minor's personal data, activity, interactions, or engagement. *Personalized Media* then prohibits using those inferences to select, recommend, rank, order, prioritize, or sequence media. Read together, the provisions could prohibit the very analysis needed to make the similar-content recommendations that the enabling statute expressly allows.[1] Accordingly, the definition should be limited to inferences used to recommend, suggest, or promote media restricted by § 2449f(a), while excluding inferences used solely for content safety, age-appropriateness, accessibility, or adaptive learning. It should also confirm that identifying "similar characteristics" for recommendations permitted by § 2449f(a)(4)(A)(iii) is not prohibited.

- ***Secondary Use***: Section 2449f(a)(2) prohibits using a covered minor's personal data for a purpose other than the purpose for which it was collected, subject to statutory exceptions. *See* 9 V.S.A. § 2449f(a)(2). The proposed definition instead treats any use not necessary to provide the service or reasonably expected by the minor as secondary, expressly including profiling, recommendations, cross-service use, advertising, and model training. That approach could prohibit activities even when the data was collected for the disclosed purpose. *Secondary Use* should use the statute's purpose-based test and define secondary use as processing for a purpose materially different from the purpose disclosed to the covered minor or parent at collection. The Attorney General should also clarify that processing for the original purpose, including maintaining, improving, or ensuring the service's safety, quality, or accessibility, is not secondary use, but necessary to provide the requested service. Likewise, the final Rule should provide clear exceptions for secondary uses that are reasonably necessary to operate and support the requested online service, product, or feature. At a minimum, permitted processing should include activities reasonably necessary to provide or maintain the

[1] The breadth of the proposed definition also raises First Amendment concerns. In *Sorrell v. IMS Health Inc.*, the Supreme Court invalidated a Vermont law that restricted the use of prescriber-identifying information for certain marketing because the law burdened speech based on its content and the identity of the speaker. 564 U.S. 552, 564–66 (2011). Similar concerns arise where a regulation restricts how a business may use lawfully held information to select or recommend content. In that context, the restriction affects not only how information is processed, but also the content ultimately presented to users. The final Rule should avoid defining prohibited data practices so broadly that it unnecessarily restricts protected expression.

service, prevent fraud, protect security and system integrity, comply with legal obligations, support internal operations, ensure accessibility, and address other routine operational, safety, or compliance needs recognized under Vermont's recently enacted privacy law. Finally, it should recognize that verifiable parental consent, as defined under COPPA (15 U.S.C. § 6501(9)), may authorize additional uses beyond the original collection purpose.

III. THE RULE CREATES A NEW GENERAL DUTY AND BROADENS THE STATUTORY FORESEEABILITY STANDARD

General Duty prohibits any data-processing or design practice that creates a "reasonably foreseeable heightened risk of harm" to a covered minor. That standard does not align with the rulemaking authority in § 2449f(b). Instead, it resembles § 2449c(b), which separately establishes a minimum duty of care for reasonably foreseeable emotional distress, compulsive use, and discrimination but does not provide an independent delegation of rulemaking authority. The result is a heightened-risk standard untethered to the specific practices and harms identified in § 2449f(b) and should be deleted.

Foreseeability raises a separate concern by expanding the statute's objective "reasonably foreseeable" standard. It adds a "knew or should have known" inquiry and identifies broad sources that may establish foreseeability, including internal testing, analytics, research, industry knowledge, guidance or standards, prior similar practices, and pre-deployment evaluations. Those sources may be relevant in some cases, but their mere existence should not establish foreseeability. Research or guidance may be disputed, methodologically weak, outdated, or unrelated to the practice or service at issue. Foreseeability should continue to be judged under the statutory "reasonably foreseeable" standard. If the Rule identifies evidence relevant to that inquiry, the evidence should be reliable, materially relevant to the specific practice and service, appropriately weighed where contested, and known or reasonably available to the covered business.

IV. THE RULE'S DATA-MINIMIZATION AND SECONDARY-USE PROVISIONS SHOULD TRACK ACT 63'S CONTEXT-SENSITIVE STANDARDS

Act 63 provides two related protections for covered minors' personal data by prohibiting: (1) a covered business from "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"; and (2) using "previously collected personal data of a covered minor for any purpose other than a purpose for which the personal data was collected, unless necessary to comply with any obligation under this chapter." *See* 9 V.S.A. § 2449f(a)(1)-(2). Those standards are context sensitive. These Rules, however, impose categorical prohibitions and obligations that exceed § 2449f and could disable service functions designed to protect or assist minors.

- ***Data Minimization***: § 2449f(a)(1) asks whether personal data is necessary to provide the "online service, product, or feature" with which the minor is actively and knowingly engaged. The Rule changes that analysis by defining "necessary to provide a service" as data "strictly required" for a "specific feature" that directly responds to an "express and unambiguous request" by the minor. *Data Minimization* goes further by extending the restrictions in § 2449f(a)(1) to retention for recommendations, analytics, and model training, and by independently prohibiting processing whenever a less data-intensive alternative is reasonably available. Taken together, the proposed framework narrows the unit of analysis from a "service" to a "feature" and add a contemporaneous-request requirement that does not appear in the statute.

  The categorical treatment of recommendations is particularly problematic for services built around them. An educational platform may need to identify appropriate material and difficulty levels, while a curated children's library may need to determine which content a child can productively engage with. In those settings, recommendation is not ancillary; it is part of the service being provided. Treating it as categorically unnecessary risks foreclosing the service model itself.

  Model training presents a different issue and should not be treated as interchangeable with deployment. Training is a backend activity, and any effect on a minor depends on how the resulting model is ultimately used. Section 2449f(a)(1) does not categorically prohibit model training. To the extent a particular use is regulated under § 2449f(b), the question is whether the deployed practice leads to compulsive use or subverts or impairs autonomy, decision making, or choice. Accordingly, "necessary to provide" should be defined consistently with the statutory phrase "necessary to provide the online service, product, or feature." Moreover, the Attorney General should clarify that recommendations may themselves be necessary for services built around content selection and model training that supports safety, content quality, or accessibility is permitted where the resulting use complies with Act 63.

  Finally, the final Rule should also recognize legitimate processing necessary to operate and support an online service. COPPA expressly recognizes processing that supports the "internal operations" of a website or online service, including activities necessary to maintain or analyze the functioning of the service, perform network communications, authenticate users or personalize content, serve contextual advertising or cap advertising frequency, protect the security or integrity of the user, website, or online service, ensure legal or regulatory compliance, and fulfill a request of a child as permitted by COPPA. See 15 U.S.C. § 6501(4); 16 C.F.R. § 312.2 (defining "support for the internal operations of the Web site or online service").

  Vermont should adopt a similarly workable approach and affirmatively permit personal data to be collected, used, retained, and disclosed where reasonably necessary to provide, maintain, protect, develop, improve, or secure the online service, product, or

feature; support internal operations; prevent fraud; ensure accessibility; or comply with applicable law. These activities are distinct from using personal data in a manner that leads to compulsive use or subverts or impairs a minor's autonomy, decision making, or choice, and should not be categorically prohibited merely because they are not tied to a specific, contemporaneous request by the minor. The Rule should also permit additional processing activities where the minor, or the minor's parent or legal guardian where appropriate, provides affirmative consent, subject to the protections and limitations established by Act 63.

- ***Secondary Use***: Section 2449f(a)(2) prohibits secondary use "for any purpose other than a purpose for which the personal data was collected, unless necessary to comply with any obligation" under Act 63. In other words, it imposes a purpose-matching test. The proposed "secondary use" definition and operative provision would extend the prohibition to profiling, recommendations, cross-service use, advertising, model training, and inferring behavioral traits, preferences, or engagement patterns to influence media, interactions, or engagement. The latter provision further states that disclosure to or consent by a covered minor does not make secondary use permissible. A business that collects data for content safety and uses profiling to detect grooming, bullying, harassment, self-harm risk, or age-inappropriate content exposure is using the data for the disclosed safety purpose, not repurposing it.

  A purpose-matching safe harbor should cover maintaining, improving, or securing a service, as well as safety, quality, or accessibility functions, when data was collected in connection with the service and the use remains consistent with the purpose disclosed at collection. The final text should also clarify that its foreclosure of minor consent does not displace verifiable parental consent obtained under COPPA, 15 U.S.C. § 6502, for specifically disclosed uses otherwise permitted under current law.

V. THE MONITORING AND CONSPICUOUS-SIGNAL REQUIREMENTS EXTEND BEYOND ACT 63 AND ROUTINE SERVICE OPERATIONS

The proposed "monitoring" definition would capture routine technical activity inherent in providing nearly any online service. Websites and applications necessarily process page requests, clicks, navigation, session information, and other interactions simply to function. Treating those activities as "monitoring" would cause ordinary service operation to trigger the Monitoring and Tracking provision's conspicuous-signal requirement.

That result is unsupported by § 2449f(a)(3), which prohibits a covered business from allowing another individual to monitor a minor's activity or location without providing a "conspicuous signal." Read in context, "monitoring" is better understood as tracking a minor, rather than every instance in which a service processes information about a user's interaction with the service. The final text should distinguish purposeful monitoring from processing necessary to

operate the service, such as loading pages, maintaining sessions, processing requests, or measuring whether a feature is functioning properly.

The proposed definition of "conspicuous signal" compounds the problem. Although the statute requires a "conspicuous signal," the Rule turns those words into nine requirements: the signal must be continuous, real-time, unavoidable, visual, displayed in the primary interface, present for the duration of monitoring, readily noticeable and understandable, and require no additional action. In practice, that amounts to a persistent user-interface requirement that the statute does not impose. Combined with the Rule's broad definition of "monitoring," the requirement could force a service to display an indicator virtually whenever it is in use. When a signal is always present, it does little to alert a minor when meaningful monitoring is occurring.

The proposed definitions and *Monitoring and Tracking* also do not account for products without a conventional visual interface. Connected toys, location devices, fitness trackers, and other screenless or limited-screen products may have no practical way to display a continuous visual indicator in a minor's "primary interface." The final text should instead require a clear and understandable signal appropriate to the product and context. Depending on the circumstances, that could include visual, audio, haptic, or device-level signals, as well as parent-facing disclosures when a persistent visual indicator is not technically feasible.

VI. THE PERSONALIZED MEDIA RESTRICTIONS FORECLOSE RECOMMENDATIONS AND USER-DIRECTED EXPERIENCES EXPRESSLY PERMITTED BY ACT 63

Section 2449f(a)(4) prohibits using a minor's personal data "to select, recommend, or prioritize media for the covered minor," subject to specific exceptions. *Personalized Media* extends that prohibition by restricting the use of behavioral data and a covered business's ability to "rank," "order," or "sequence" media for a covered minor. These additions expand the statutory prohibition without support in the enabling statute. The prohibition should therefore adhere to the statutory text, and clarify that "personal data or behavioral data" in this provision means the covered minor's own data used to personalize media for that covered minor.

The exceptions require similar revisions. 9 V.S.A. § 2449f(a)(4)(C) permits personalized media that shares "similar characteristics as the media [covered minors] are currently viewing." Subsection (b) of the Rule, however, prohibits personalization based on "prior interactions" or "viewing history." Those restrictions could prevent a service from making the limited inferences necessary to identify similar media and give effect to the statutory exception. That exception should be preserved, with limited use of recently viewed content permitted where necessary to identify comparable media and provide continuity. The final Rules should confirm that a covered minor's affirmative, in-session action—such as selecting "more like this," choosing a title to view, or otherwise affirmatively initiating playback—may constitute an express and unambiguous request under § 2449f(a)(4)(A)(iii) for similar-characteristic recommendations within that session, without authorizing persistent cross-session preference inference.

Lastly, the proposed definition of "express and unambiguous request" creates additional practical problems for services designed for children. *Personalized Media* Subsection (d) permits media displayed in response to a minor's request for a particular account, category, or type of media. The definition, however, requires a "specific and contemporaneous" request that cannot be inferred from prior activity, behavioral data, or persistent interaction patterns. The final text should clarify that the request may come from the minor or their parent or guardian. The final text should also allow a one-time affirmative setup or configuration choice to be sufficient where it reasonably reflects the user's or parent's continuing instruction, rather than requiring a fresh request before each content interaction. Indeed, children, particularly pre-literate users, may express what they want to see through affirmative selections, repeated viewing, or other age-appropriate interactions rather than a typed or verbal request. Educational services may adjust content or difficulty based on demonstrated performance, while children's media services may organize a finite catalog by age range, accessibility setting, or a user-selected category. Services may also filter or de-prioritize age-inappropriate material for safety reasons.

The final text should account for these ordinary and beneficial functions. It should clarify that adaptive learning, safety filtering, accessibility features, finite human-curated catalogs, bounded playlists, user-initiated watchlists or favorites, and other age-appropriate means of responding to a minor's choices remain permissible.

VII. INCREASED ENGAGEMENT ALONE DOES NOT ESTABLISH COMPULSIVE USE UNDER ACT 63

The provision sweeps more broadly than the enabling statute by treating increased engagement as evidence of compulsive use without requiring a connection to the statutory harm. Section 2449a(8) defines "compulsive use" as repetitive use that "materially disrupts" a minor's major life activities. *See* 9 V.S.A. § 2449a(8). Increased time spent, session length, or frequency of use may be relevant to that analysis, but those metrics alone do not establish compulsive use.

That distinction matters because many ordinary product features may increase interaction precisely because they make a service more useful. A better search function may cause a minor to use an educational service more frequently; faster loading times may allow a user to remain on a service longer; and more relevant or higher-quality content may increase interaction without disrupting any major life activity. *Compulsive Use*, however, treats those outcomes as evidence of compulsive use and, in some cases, creates a rebuttable presumption based on ordinary practices such as recommendations, behavioral signals, or engagement-based ranking.

The final text should instead require a causal nexus between the challenged practice and the statutory standard of "material disruption." Rather than cover practices merely "designed or reasonably likely to increase, prolong, or intensify" interaction, it should focus on practices that drive engagement beyond a minor's intent or awareness and are reasonably likely to materially disrupt a major life activity and clarify that increased engagement resulting from improvements to content quality, relevance, functionality, or usability does not, by itself, constitute compulsive use.

VIII. ORDINARY DESIGN INFLUENCE DOES NOT CONSTITUTE AN IMPAIRMENT OF AUTONOMY UNDER ACT 63

The Rule treats broadly defined forms of influence as evidence of impairment, including practices that "materially steer" a minor's choices or rely on "behavioral, psychological, or cognitive influence techniques." It therefore scopes in ordinary and beneficial design choices. Every interface necessarily influences how users interact with a service through the placement and sequencing of information and the presentation of available choices. A service may prominently display a privacy-protective option or prioritize age-appropriate or educational content. Those practices may "steer" a minor, but they do not necessarily subvert or impair the minor's ability to choose. The relevant issue is whether a practice "materially interferes" with the minor's ability to make an informed and voluntary decision, not simply whether the design influences that decision.

An appropriate final rule would distinguish beneficial design from practices that manipulate a minor in a manner that meaningfully impairs decision making or choice. Practices that obscure material information, interfere with controls, impose unreasonable barriers to disengagement, or otherwise prevent a minor from making an informed and voluntary choice may appropriately fall within the provision. Good-faith design choices that guide children toward safe or educational outcomes, by contrast, should not be deemed autonomy impairments.

The rebuttable presumptions raise a separate concern and should be deleted. Subsection (c) would presume an impairment of autonomy based on certain defined practices, while subsection (d) would require a covered business to overcome that presumption through "clear and convincing evidence." Section 2449f(b) directs the Attorney General to identify and prohibit practices that subvert or impair autonomy, but it does not establish a rebuttable presumption or authorize a heightened evidentiary standard.

IX. THE PROPOSED DESIGN PROHIBITIONS EXTEND BEYOND THE PRACTICES AND HARMS IDENTIFIED IN ACT 63

Several proposed prohibitions extend beyond practices expressly addressed by Act 63. Where the Act does not independently prohibit a particular practice, the Rule should remain tied to § 2449f(b) and to whether the practice "lead[s] to compulsive use or subvert[s] or impair[s] user autonomy, decision making, or choice." The provisions discussed below could prohibit practices without a sufficient connection to those statutory harms, including practices that serve legitimate educational, safety, functional, or user-directed purposes.

- ***Autoplay*:** Because Act 63 does not independently prohibit autoplay, any restriction must be tied to § 2449f(b). Not every form of autoplay leads to compulsive use or subverts or impairs a minor's autonomy, decision making, or choice. A parent may, for example, affirmatively enable autoplay for a curated children's playlist, a sequence of educational programming, or music during a car trip. In those circumstances, automatic

playback does not necessarily encourage compulsive use or interfere with a minor's decision making. A categorical prohibition would also prevent parents from choosing how their children use a service, even when autoplay has been affirmatively enabled through parental controls.[2] Any restriction should focus on forms of autoplay with a demonstrated connection to the harms addressed by § 2449f(b). At minimum, autoplay should be permitted when a parent has affirmatively enabled the feature through parental controls, with infinite or algorithmically generated feeds distinguished from finite, curated playlists or sequentially ordered content.

- ***Behavioral Recommendation Systems***: Section 2449f(a)(4) governs when personal data may be used to recommend media to minors and when personalized media remains permissible. The provision expands that framework by separately prohibiting the use of "behavioral data" or "inferred preferences" to rank, order, or sequence media and by declaring that all such systems "rely on engagement optimization" and operate without an "express and unambiguous request." As a result, it applies to systems serving educational, safety, organizational, and other non-engagement purposes, such as adapting material based on performance, directing minors away from inappropriate content, or surfacing recently viewed or affirmatively selected content. The prohibition on "ranking" or "ordering" may likewise reach ordinary library functions even when the service does not seek to maximize engagement. The provision's categorical treatment of these systems as operating without a minor's request also fails to account for recommendation features that a minor affirmatively chooses to use, such as a music-discovery feature or reading list.

  The final text should track the scope and exceptions in § 2449f(a)(4), rather than expand the prohibition through additional categories. It should remove the categorical treatment of recommendation systems as engagement optimization and clarify that educational and safety recommendations, finite curated catalogs, recommendations based on non-personal, aggregate, or context-ranking signals, and content organized based on a minor's affirmative selections are not prohibited when otherwise consistent with the statute.

- ***Circumvention***: Although anti-circumvention provisions are common in regulatory frameworks, the proposed standard is broader because it prohibits any alternative practice that produces "substantially similar effects." Similar engagement outcomes do not necessarily mean that a business has circumvented a prohibited practice. For example, if a business replaces a prohibited algorithmic recommendation system with

[2] Parents have a constitutionally protected interest in directing the care and upbringing of their children, including a presumption that fit parents act in their children's best interests. *See Troxel v. Granville*, 530 U.S. 57, 65–69 (2000) (holding there is a fundamental right under the Fourteenth Amendment for a parent to oversee the care, custody, and control of a child). A rule that overrides parental configuration choices impairs the very autonomy that § 2449f(b) is supposed to protect, namely, parental autonomy.

human editorial curation, the curated content may similarly increase engagement because users find it relevant or useful. Under the proposed standard, however, that practice could be deemed circumvention because it achieves "substantially similar effects through alternative means," even though human editorial judgment does not replicate the prohibited recommendation mechanism.

The "substantially similar effects" standard also makes it difficult to determine before deployment whether a new feature complies with the Rule, because its effects may become apparent only after the feature is tested or used. Any final rule should require that a practice be designed or deployed *with the intent* to evade a specific prohibition. It should also clarify that legitimate alternative designs do not constitute circumvention merely because they increase engagement and provide an opportunity to cure when a good-faith practice is later determined to produce prohibited effects.

- ***Continuous Media Feeds***: The provision treats infinite feeds and bounded content libraries alike based on how media is loaded or displayed. The concerns presented by an endless generated feed differ from those presented by a finite catalog with a defined endpoint. A children's streaming service, for example, may automatically load additional titles as a minor scrolls through an age-appropriate library. Although the stream provides additional media, it has a defined endpoint. The final text should target feeds that eliminate meaningful stopping points in a manner that contributes to the harms identified in § 2449f(b). Finite catalogs, curated libraries, and other bounded collections should not be prohibited merely because scrolling, swiping, or automatic loading is used to navigate them.

- ***Engagement-Based Notifications***: The provision does not distinguish notifications intended to drive engagement from those providing functional or time-sensitive information. A notification that a library book is due, a bus is arriving, a class is beginning, or an appointment is approaching may be triggered by a minor's prior activity and prompt the minor to return to an online service. Its purpose, however, is to convey useful information, not to prolong or reinitiate engagement. Treating those communications the same as prompts designed to draw minors back to a service after disengagement extends the prohibition beyond the harms addressed by § 2449f(b). The prohibition should focus on notifications whose primary purpose is to drive or prolong engagement and distinguish them from communications serving functional, educational, safety, or other informational purposes. It should also expressly preserve parent-configured notifications and clarify that notifications conveying time-sensitive information tied to real-world events are not "engagement-based" merely because they reference the child's prior activity.

- ***Push Notifications***: Section 2449f(a)(5) prohibits sending push notifications to a covered minor between 12:00 midnight and 6:00 a.m., but the provision effectively extends that restriction to all hours by prohibiting notifications based on personal or behavioral data

or inferred preferences. That prohibition could capture routine notifications that necessarily rely on information about the recipient, such as package-delivery updates and library due-date reminders, even when they convey useful information rather than drive "repeated, prolonged, or compulsive engagement." The statutory midnight-to-6:00 a.m. restriction should remain the baseline rather than be replaced by a broader categorical ban. Any additional restrictions should distinguish notifications designed to manipulate engagement from those serving a functional purpose and preserve notifications configured by a parent, tied to real-world events, or affirmatively requested by a minor or parent.

- ***Reinforcement Mechanisms***: The provision prohibits variable or intermittent rewards, including "likes, badges, or points" and "gamified incentives," without requiring a connection to compulsive use as defined by § 2449a(8). These mechanisms may, in some cases, promote the major life activities the statute seeks to protect. Reading badges, educational mastery points, language-learning achievements, and savings-goal milestones, for example, can encourage reading, learning, concentration, or financial literacy. Treating those features as equivalent to reward mechanisms that "materially disrupt[]" major life activities fails to account for differences in their purpose and practical effect. The final text should distinguish mechanisms that drive excessive engagement from those that support educational progress, financial literacy, health or fitness goals, or other beneficial activities, and preserve the latter where they do not contribute to compulsive use.

- ***Social Pressure Features***: The provision prohibits features that create "social pressure, urgency, or perceived obligation" to engage, but social interaction does not necessarily impair autonomy or contribute to compulsive use. Class reading challenges, collaborative learning, peer tutoring, and group fitness challenges may use social encouragement or shared progress to motivate beneficial activities. For example, showing a class's collective reading progress or allowing members of a youth running club to track shared goals may encourage continued participation without producing the harms addressed by § 2449f(b). The final text should distinguish features that exploit negative social dynamics, such as shame, exclusion, or anxiety about belonging, from educational, fitness, peer-support, and similar features that use social interaction to encourage positive participation.

X. THE RULES SHOULD BE HARMONIZED WITH VERMONT'S EXISTING PRIVACY LAWS

Neither Act 63 nor the proposed Rules explain how their requirements interact with Vermont's student privacy law, 9 V.S.A. §§ 2443 et seq. ("Act 89"), or the Vermont Data Privacy and Online Surveillance Act, 9 V.S.A. §§ 2415a et seq. ("Act 145"). Without greater clarity, businesses may be subject to different Vermont standards governing the same processing activity.

Act 89 presents the clearest example in the educational context. Vermont already regulates operators of online services designed and marketed for PreK-12 school purposes. *See* 9 V.S.A. § 2443(2)–(4). The Legislature expressly preserved uses of student data to maintain, develop, support, improve, or diagnose an online service, *id*. § 2443a(b), for qualifying research, *id*. § 2443c(2), and for recommendation engines that provide additional educational, learning, or employment content and services, *id*. § 2443d(4). Act 89 also expressly provides that it does not limit the use of student data for "adaptive learning or customized student learning purposes." *Id*. § 2443e(2). The Rules could restrict those same practices by limiting "necessary" processing to what is "strictly required" for a specific feature directly responsive to a minor's express and unambiguous request and restricting recommendations, certain analytics, profiling, and model training or development. An adaptive-learning platform, for example, may use a student's prior performance to adjust difficulty or recommend the next lesson without requiring a separate express request for each adjustment. Act 89 expressly accommodates that use, while the Rules prohibit it. The final Rules should address that overlap and clarify that educational practices expressly permitted under Act 89 are not categorically prohibited under the AADC.

Act 145 creates a similar issue. It requires controllers to limit collection to what is "reasonably necessary and proportionate" to disclosed purposes and permits processing for a material new purpose when the purpose is reasonably necessary to or compatible with the original purpose or the consumer provides consent. *See* 9 V.S.A. § 2415e(a)(1)–(2). The Rules instead limit necessary processing to what is "strictly required" for a specific feature directly responsive to an express and unambiguous request and prohibit secondary uses even when disclosed to or consented to by the covered minor. The Rules therefore replace Act 145's proportionality, compatibility, and consent framework with a substantially narrower standard for covered minors.

Accordingly, the final Rules should harmonize the AADC with these existing statutory frameworks and clarify that practices expressly permitted under Act 89 or otherwise permissible under Act 145 are not categorically prohibited under the AADC unless they create the harms enumerated in 9 V.S.A. § 2449f(b).

* * *

Proposed Rule 26P027 can advance meaningful protections for minors while remaining grounded in the framework enacted by the Legislature. SPSC appreciates the Attorney General's work to develop clear and workable requirements that can be implemented in practice.

We appreciate your office's time and consideration and stand ready to work collaboratively on rules that achieve durable, enforceable, and balanced protections for Vermont's minors.

Respectfully submitted,



Andrew A. Kingman
Counsel, State Privacy & Security Coalition



William C. Martinez
Counsel, State Privacy & Security Coalition

STATE PRIVACY & SECURITY COALITION

October 2, 2026

The Honorable Charity R. Clark
Office of the Vermont Attorney General
109 State Street
Montpelier, VT 05609

RE: Proposed Rule 26P028 - Vermont Age-Appropriate Design Code

Dear Attorney General Clark:

The State Privacy & Security Coalition (SPSC) is a multi-sector coalition representing over 30 companies and seven trade associations across the retail, technology, telecommunications, healthcare, automotive, and payment card sectors. We appreciate the opportunity to comment on Proposed Rule 26P028 (Age Assurance Privacy) and the Attorney General's efforts to obtain stakeholder input before the rules take effect.

Act 63 directs the Attorney General to identify commercially reasonable and technically feasible age-assurance methods while prioritizing privacy and accessibility over accuracy. Several provisions of the proposed Rule go further, including by requiring age assurance based on likely access by minors, restricting reuse of age-range determinations, and establishing assessment and documentation requirements not expressly provided by the statute.

The implementation timeline is also a significant concern. The Proposed Rules contemplate substantial changes to existing products, data-processing practices, and technical systems, including requirements concerning monitoring and tracking, personalized media and recommendation systems, age assurance, data minimization, and third-party practices. Businesses will need time after the Rules are finalized to determine which products and features are affected, modify technical systems and product functionality, coordinate with vendors and service providers, update compliance processes, and test those changes before deployment. These steps cannot reasonably be completed until businesses know the standards ultimately adopted by the Attorney General. With the Proposed Rules currently providing for a January 1, 2027 effective date, the final Rules should provide businesses at least 12 months from publication of the finalized Rules to come into compliance with the new requirements.

Our comments recommend targeted revisions to preserve Act 63's privacy-first approach and avoid requirements that could result in more intrusive or duplicative data collection. The final Rule should allow businesses to use proportionate age-assurance methods, act on valid age-range determinations, correct and evaluate errors, and protect age-assurance data without unnecessarily expanding the collection of personal information.

I. THE RULE CREATES AN AGE-ASSURANCE REQUIREMENT NOT FOUND IN ACT 63

Section 2449g(a) imposes obligations on covered businesses and processors "[d]uring the process of conducting age assurance," while § 2449g(b) directs the Attorney General to identify "commercially reasonable and technically feasible" age-assurance methods. Neither provision expressly requires a covered business to conduct age assurance. The provision, however, requires businesses to implement age assurance for any service, product, or feature "reasonably likely to be accessed by covered minors." That standard encompasses virtually any general-audience online service, including search engines, streaming services, weather and news sites, e-commerce platforms, and email services, simply because minors may access them. In practice, the Rule could require age assurance across a substantial portion of the general-audience internet, despite the Legislature's intent to do so.

That expansion is particularly significant because age assurance is not a costless compliance measure. Regulators considering age assurance have recognized that these technologies can impose privacy and security risks, create accessibility and accuracy concerns, introduce friction for lawful users, and require businesses to collect or process information they otherwise would not need. Australia's eSafety Commissioner, for example, has emphasized that age-assurance measures should be proportionate to the particular risk and has cautioned against a one-size-fits-all technological approach.[1] European regulators have likewise taken a risk-based approach, recommending age verification for legally age-restricted content and services and where identified risks to minors cannot be mitigated through less intrusive measures.[2] These approaches underscore the consequences of interpreting the Rule to impose age assurance based solely on the likelihood that a minor may access a service, without regard to the nature of the service or the risk it presents.

The statutory framework should govern when these requirements apply: they should attach when a covered business conducts age assurance, not merely because a service is reasonably likely to be accessed by minors. At a minimum, "reasonably likely to be accessed by covered minors" should be limited to services directed to minors or services in which minors constitute a substantial portion of the actual user base, rather than any service a minor could theoretically access.

II. THE ACCURACY REQUIREMENTS CONFLICT WITH ACT 63'S PRIVACY-FIRST APPROACH TO AGE ASSURANCE

The Rule's accuracy requirements create tension with the enabling statute's mandate to "prioritize user privacy and accessibility over the accuracy of age assurance methods." 9 V.S.A. §

[1] *See* Julie Inman Grant, eSafety Comm'r, *A Matter of Principle: Guiding the Age Verification Roadmap* (Jan. 19, 2023), https://www.esafety.gov.au/newsroom/blogs/a-matter-of-principle-guiding-the-age-verification-roadmap.
[2] *See* Eur. Comm'n, *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* § 6.1.3 (July 14, 2025), https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors.

2449g(b)(2)(A). *Graduated Escalation* subsection (a) requires businesses to begin with less intrusive methods, including self-declaration with "reasonable safeguards," but *Accuracy and Error Evaluation* subsection (c) prohibits an age-assurance method when its error rate creates a "material risk" of misclassifying minors. The provisions neither define what level of error constitutes a "material risk" nor explains what "reasonable safeguards" make self-declaration sufficient. Without clarification, businesses may have to begin with a privacy-protective method only to conclude that its error rate requires escalation to a more intrusive method. That result is contrary to the legislative intent. The final Rule should state expressly that lower accuracy is acceptable when the alternative is more intrusive data collection, define reasonable safeguards for self-declaration, and explain when escalation is required. Alternatively, the accuracy requirement should apply to the age-assurance process, including escalation and fallback mechanisms, rather than require each individual step to satisfy the same standard independently. Additionally, the final rules should acknowledge adult-owned family account structures as a valid form of age verification across all associated sub-profiles.

Subsection (d) also requires businesses to evaluate whether error rates disproportionately affect groups of minors. Conducting that analysis may itself require demographic information, such as race, ethnicity, gender, or disability status, that a business would not otherwise collect. This creates tension with *Data Minimization*, which limits collection to data "strictly necessary to provide the service." Demographic data is not necessary to make the age determination, but it may be necessary to evaluate fairness. A safe harbor should allow businesses to collect demographic data solely to evaluate and mitigate bias in age-assurance methods.

III. THE PROHIBITED-USE AND DATA-MINIMIZATION REQUIREMENTS EXTEND BEYOND ACT 63 AND COULD REQUIRE DUPLICATIVE DATA COLLECTION

Section 2449g(a) applies to "covered businesses and processors," and § 2449a(23) defines a processor as a person that processes personal data on behalf of a covered business. *Prohibited Uses*, however, requires covered businesses to impose age-assurance restrictions by contract on third parties and vendors regardless of whether they qualify as processors under Act 63. That requirement extends the Rule beyond the entities identified by the Legislature. The final text should conform to the statutory scope by applying these requirements to entities that qualify as processors under Act 63, rather than extending them to other third parties through mandatory contractual terms.

Data Minimization and *Prohibited Uses*, read together, could also require businesses to collect the same age information more than once. *Data Minimization* prohibits using age-assurance data for "any secondary purpose," while *Prohibited Uses* permits such data to be used only to determine whether a user is a covered minor and specifically bars its use for personalization, recommendation systems, profiling, or inferring additional characteristics, behaviors, or preferences.

Those restrictions may prevent businesses from using age information already obtained through age assurance for legitimate age-related service functions. An educational service, for example, may need age information to provide grade-appropriate material, while other services may use age to apply age-appropriate content restrictions, privacy settings, or safety features. If age information obtained through age assurance cannot also be used for those purposes, a business may have to collect the same information twice. That result increases the amount of data collected, contrary to data minimization principles.

The prohibition on personalization and recommendation systems presents a similar issue. For some services, personalization is not an ancillary feature but an integral part of the service itself. Streaming, educational, music, news, and other content-based services rely on recommendations to organize large catalogs and help users navigate and discover relevant content. A categorical prohibition does not distinguish those ordinary functions from recommendation practices that present a material risk to minors.

The final Rule should distinguish repurposing age-assurance data for unrelated purposes from using an age or age-range determination for legitimate service functions. A risk-based approach would preserve restrictions on personalization and recommendation practices that present a material risk to minors without sweeping in functionality that is necessary or integral to a service requested by the user. At a minimum, the Rule should permit use of an age or age-range determination to provide age-appropriate content, features, recommendations, and protections; comply with age-based legal requirements; and support personalization or recommendation functionality that is necessary or integral to the service requested by the user, without requiring the business to collect the same information a second time.

IV. THE LINKABILITY RESTRICTIONS COULD INCREASE DATA COLLECTION AND EXTEND BEYOND AGE-ASSURANCE DATA

Section 2449g(a)(2) requires covered businesses to delete personal data collected for age assurance immediately after determining whether a user is a covered minor but permits retention of "the determination of the user's age range." Subsection (a) would restrict use of that retained determination across services, accounts, or contexts, undermining data minimization. When a covered business has already determined a minor's age range, requiring a new age-assurance process when the same user accesses another service, device, or context may require additional personal-data collection that would otherwise be unnecessary. A minor, for example, could be required to repeat age assurance when accessing another service offered by the same covered business, even when the existing determination provides the necessary level of assurance.

Reuse of a retained age-range determination within the same covered business and among affiliated services should be permitted when the prior determination provides the level of assurance required for the subsequent use. The limitation that permits reuse only where it is "strictly necessary to prevent circumvention" should be removed. A valid age-range

determination should be reusable for age-assurance purposes when it provides the required level of assurance, avoiding unnecessary additional collection from the minor.

Subsection (b) raises a separate concern by prohibiting the use of persistent identifiers or other techniques that "enable cross-service, cross-context, or cross-device tracking of a covered minor," regardless of whether those identifiers are used for age assurance. Persistent identifiers, including account identifiers, session tokens, and device identifiers, support ordinary service functions such as authentication, parental controls, and synchronization across devices. Section 2449g(b)(1) authorizes rules identifying age-assurance methods and providing additional privacy protections for age-assurance data; it does not extend that authority to persistent identifiers used for purposes unrelated to age assurance. As written, the provision could restrict common account and service functionality simply because an identifier allows a minor to be recognized across services or devices. The prohibition should be limited to identifiers collected or generated for age assurance and later repurposed for unrelated cross-service, cross-context, or cross-device tracking, while preserving the use of those identifiers for ordinary service operation, account management, and parental controls.

The prohibitions on using age-assurance data for recommendation systems raise a related problem. Once a service determines a user's age range, it may need to act on that determination to provide an age-appropriate experience, such as by providing appropriate content or managing access restrictions. A categorical prohibition could prevent use of the retained age-range determination for those purposes and instead require a business to obtain the same information through another means. Using an age-range determination to provide an age-appropriate experience within a service is materially different from using age-assurance data to profile a minor or track the minor across contexts. The final text should distinguish between those activities and permit use of an age-range determination to provide age-appropriate content, features, protections, and access controls, while maintaining the statute's restrictions on repurposing the underlying personal data collected to perform age assurance.

V. THE APPEALS PROCESS SHOULD PRESERVE FLEXIBLE METHODS FOR CORRECTING AND EVALUATING INACCURATE AGE DETERMINATIONS

Subsection (e)(4) prohibits the "use of a highly intrusive age assurance process or technique as a condition of appeal where less intrusive alternatives are reasonably available and sufficient." This subsection should not be interpreted to prevent a minor from voluntarily using a more reliable age-assurance method to correct an inaccurate determination. An initial determination may be based on a less intrusive method that produces an incorrect result, while resolving the appeal may require different or additional information. For example, a 17-year-old incorrectly identified as a younger minor should be permitted to choose to provide identification or use another higher-confidence method to establish the correct age. The final text should clarify that a more intrusive method may be offered as an optional means of resolving an appeal when proportionate to the need for an accurate determination, while preserving the prohibition

against requiring that method when a less intrusive alternative is reasonably available and sufficient.

The Rule should also allow covered businesses to evaluate why inaccurate determinations occur and improve their age-assurance systems. Section 2449g(a)(2) requires deletion of personal data collected for age assurance once the age determination is made, limiting the ability to retain the underlying data for subsequent error analysis. The final text should therefore clarify that covered businesses may retain non-identifying information about erroneous determinations and appeal outcomes, consistent with the statute's deletion requirements, for the limited purposes of measuring accuracy, identifying recurring errors, and reducing future misclassifications.

VI. THE COMPLIANCE AND OVERSIGHT REQUIREMENTS CREATE AN ASSESSMENT REGIME AND REBUTTABLE PRESUMPTIONS NOT FOUND IN ACT 63

The provision creates a detailed assessment and documentation regime not required by § 2449g. Covered businesses would have to conduct assessments before deploying or materially modifying an age-assurance process, evaluate eight categories of risks and considerations, maintain specified documentation, and periodically update those assessments. Failure to maintain the required documentation would create a rebuttable presumption of noncompliance, while use of a highly intrusive age-assurance method without documented justification would create a rebuttable presumption of violation.

Those requirements extend beyond the authority delegated by § 2449g(b). The statute authorizes the Attorney General to identify commercially reasonable and technically feasible age-assurance methods, describe appropriate review processes, and provide "additional privacy protections for age assurance data." Although that authority permits rules governing the collection, use, retention, disclosure, and protection of age-assurance data, it does not expressly authorize a separate assessment framework. Where state legislatures have intended to require formal data-protection impact assessments, they have done so expressly.[3]

The rebuttable presumptions in subsections (g) and (h) raise an additional concern. Section 2449h establishes the consequences of violating the statute and provides for enforcement under Vermont's Consumer Fraud Act, but it does not authorize evidentiary presumptions based on a business's failure to retain specified documentation. The new documentation requirement should not be converted into a presumption that the underlying substantive requirements have been violated.

[3] *See, e.g.*, Md. Code Ann., Com. Law § 14-4804(a)(1) ("A covered entity that provides an online product reasonably likely to be accessed by children shall prepare a data protection impact assessment for the online product."); Cal. Civ. Code § 1798.99.31(b) ("The Data Protection Impact Assessment required by this paragraph shall identify the purpose of the online service, product, or feature, how it uses children's personal information, and the risks of material detriment to children that arise from the data management practices of the business.").

The mandatory assessment framework and rebuttable presumptions should be removed. If documentation requirements are retained, they should be limited to records reasonably necessary to demonstrate compliance with the protections for age-assurance data authorized by § 2449g. Any remaining requirements should also account for the "size, financial resources, and technical capabilities" of covered businesses, as § 2449g(b)(2)(B)(i) expressly requires.

* * *

Proposed Rule 26P028 can provide meaningful protections for minors while remaining grounded in the framework enacted by the Legislature. SPSC appreciates the Attorney General's consideration of these comments and welcomes the opportunity to work toward clear, workable, and balanced final rules.

Respectfully submitted,



Andrew A. Kingman
Counsel, State Privacy & Security Coalition



William C. Martinez
Counsel, State Privacy & Security Coalition

Bambara, Anthony

Subject: Vermont AADC Rulemaking - Entertainment Software Association (ESA) Comments

From: Michael Lewis <MLewis@theesa.com>
Sent: Friday, October 2, 2026 3:14 PM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Cc: Michael Lewis <MLewis@theesa.com>
Subject: Vermont AADC Rulemaking - Entertainment Software Association (ESA) Comments

Some people who received this message don't often get email from mlewis@theesa.com. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Dear Attorney General Clark,

On behalf of the Entertainment Software Association (ESA), attached please find ESA's comments regarding the proposed implementing rules for the Vermont Age-Appropriate Design Code Act. We would be happy to answer any questions regarding our submission or arrange a meeting to discuss our comments further. Thank you.

Best,

Michael G. Lewis
VP and Associate General Counsel, Law and Policy

601 Massachusetts Avenue NW | Suite 300 | Washington, DC 20001
mlewis@theesa.com | P: 202.903.2400 |
Entertainment Software Association | www.theESA.com

October 2, 2026

Attorney General's Office
ATTN: Vermont Age-Appropriate Design Code Act
109 State Street
Montpelier, VT 05609

Comments of the Entertainment Software Association
Regarding the Vermont Age-Appropriate Design Code Rulemaking

The Entertainment Software Association[1] ("ESA") appreciates the opportunity to submit comments regarding the Vermont Attorney General's Office's ("AGO") proposed rules under the Vermont Age-Appropriate Design Code Act ("AADC").[2] As discussed in our March comments, ESA shares the AGO's interest in promoting policies that will allow Vermonters of all ages to enjoy access to online experiences that are safe, fun, and rewarding.[3] ESA respectfully provides the following comments to help the AGO develop policies that will advance these important policy goals.

As expressed in our March comments, to keep kids safe online, in our experience it is important for regulations to be flexible and proportionate and to help parents decide what is right for their families. We recommend that the AGO remove the proposed age assurance mandate because such requirements go beyond the authority granted in the AADC and would prompt unnecessary collection of personal information. We also recommend clarifying the limits on the use of age information to allow for beneficial safety purposes beyond age assurance and updating the proposed rules to ensure that any deletion requirements allow for reasonable safety operations (and avoid creating user friction that could undermine safety). Additionally, we suggest modifying the rules regarding monitoring and notifications to reduce potential user confusion and ensure that basic game functionality, including safety functions, are not unintentionally impeded. Further, we suggest stronger measures to protect content and expressive activity under the First Amendment. We would be glad to discuss these views and our experience with the AGO.

---

[1] ESA is the U.S. trade association for companies that publish interactive entertainment software for video game consoles, handheld devices, personal computers, and the internet. Our members not only create some of the world's most engaging interactive experiences for consumers, but also develop novel technologies that are at the cutting edge, such as virtual, augmented, and mixed reality hardware and software as well as the latest consoles and handheld video game devices.

[2] Vt. Age-Appropriate Design Code Rulemaking, Off. of the Vt. Att'y Gen., https://ago.vermont.gov/vermont-age-appropriate-design-code-rulemaking.

[3] Comments of the Ent. Software Ass'n, Age-Appropriate Design Code Rulemaking Feedback (Mar. 16, 2026), https://ago.vermont.gov/sites/ago/files/2026-08/ESA%20Vermont%20AADC%20Comments%20-%20%203.16.2026%20(final-signed)%20(1).pdf.

I. Video games are a popular pastime for Vermonters of all ages and from all backgrounds.

Research shows that people from all walks of life play video games for fun, and that video games can benefit a person's mental, emotional, and social well-being in remarkable ways, as discussed in our March comments. Our subsequently released 2026 industry report affirms these benefits, including the reasons why parents appreciate video games.[4]

Our prior comments noted the popularity and wide-ranging benefits of video games for users. For many households, playing video games has become a regular and invaluable way to engage, upgrading passive screen time with memorable moments for adults and kids alike. For example, two-thirds of Americans – people of all ages, ethnicities, races, gender identities and backgrounds – play video games.[5] An Oxford University study involving more than 80,000 players reported that their findings "corroborate what qualitative research and reports from video game players around the world have long suggested: people feel good playing games."[6] Other research has noted that "video gameplay gives gamers the chance to develop techniques for dealing with conflict, working out various resolutions, interacting with their friends, and experiencing different emotions"[7] and that "[c]ognitive skills such as perception, attentional control, and decision-making improve when subjects were trained with video games."[8] We also noted that video games are a unique medium that can empower players to visualize themselves in a story, which can be especially powerful for players from underrepresented backgrounds.[9]

ESA's 2026 industry report further illustrates how Vermonters turn to video games to relax, unwind, and connect with friends and family. Year after year, we see Americans shaking up stereotypes about who is and who can be a "gamer." Today, more than 212.3 million Americans play video games regularly, including men and women at nearly equal rates and

---

[4] ESA, 2026: Essential Facts About the U.S. Video Game Industry, https://www.theesa.com/wp-content/uploads/2026/06/2026-Essential-Facts-Booklet-05-27-26.pdf.

[5] *Inclusion and Belonging*, Ent. Software Ass'n, https://www.theesa.com/issues/inclusion-belonging.

[6] ESA, Power of Play: 2025 Global Video Games Report (2025), https://www.theesa.com/resources/the-global-power-of-play-report (quoting Vuorre, M., Ballou, N., Hakman, T., Magnusson, K., & Przybylski, A. K. (2023). Affective uplift during video game play: A naturalistic case study. [PREPRINT]); *see also id.* ("[G]aming may be among the most efficient and effective means by which children and youth generate positive feelings.") (quoting Granic, I., Lobel, A., & Engels, R. C. (2014). The benefits of playing video games. *American Psychologist*, 69(1), 66–78)).

[7] ESA, Power of Play: 2025 Global Video Games Report (2025), https://www.theesa.com/resources/the-global-power-of-play-report (quoting Markey, P. M., Ferguson, C.J., & Hopkins, L.I. (2020). Video game play: Myths and benefits. *American Journal of Play*, 13(1), 87–106)).

[8] ESA, Power of Play: 2025 Global Video Games Report (2025), https://www.theesa.com/resources/the-global-power-of-play-report (quoting Reynaldo, C., Christian, R., Hosea, H., & Gunawan, A. A. S. (2021). Using video games to improve capabilities in decision making and cognitive skill: A literature review. *Procedia Computer Science*, 179, 211–221)).

[9] *Inclusion and Belonging*, Ent. Software Ass'n, https://www.theesa.com/issues/inclusion-belonging.

players from every generation.[10] The top two reasons that Americans play video games are to relax and to have fun.[11] Older generations also like to play to keep their minds sharp.[12] These findings affirm the appeal of video games and their wide-ranging benefits.

This report also notes that 75% of parents play video games, and of those who do, 81% have played video games with their children.[13] A majority of these parents reports that they play video games with their children because it is fun for the whole family, a good opportunity to socialize, and a great way for the family to spend time together.[14] More than 7 in 10 parents prefer their child to spend time playing video games than on social media and say playing video games offers more potential benefits for their children compared to social media.[15] These findings demonstrate the appeal of video games for families and how parents take an active role in their children's video game experiences.

II. The video game industry employs leading protections for privacy and online safety.

The video game industry is proud to have implemented leading consumer privacy and online safety measures, as also discussed in our March comments. Indeed, the Federal Trade Commission ("FTC") has lauded the industry's efforts on these fronts and noted that the video game industry "outpaces" other entertainment sectors in having the "strongest self-regulatory code" and "high compliance" with that code.[16] Our subsequently released 2026 industry report underscores how families value these measures to help ensure that children have safe and positive experiences playing video games.

For example, the Entertainment Software Rating Board ("ESRB"), the video game industry's self-regulatory body since 1994, operates Privacy Certified, a privacy compliance and certification program, which offers two seals that certify a member's compliance with digital privacy laws. These are the ESRB Privacy Certified Seal ("General Seal")—for video game products and services aimed at adults, including those used by teens—and Kids Seal, for such offerings directed or targeted to children. The FTC has approved the Kids Seal as a Children's Online Privacy Protection Act ("COPPA") Safe Harbor Program.[17]

---

[10] ESA, 2026: Essential Facts About the U.S. Video Game Industry, https://www.theesa.com/wp-content/uploads/2026/06/2026-Essential-Facts-Booklet-05-27-26.pdf.

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Player Safety*, Ent. Software Ass'n, https://www.theesa.com/issues/player-safety.

[17] *Id.*

Both the General and Kids Seals incorporate a range of important privacy and safety standards. The General Seal Requirements are based on federal and state laws, regulatory enforcement, and best practices, incorporating principles such as transparency and notice, consent and choice, data minimization, and accountability. For General Seal approval, companies must give consumers clear and accurate information regarding (i) how their personal information is collected, used, and shared, and (ii) how to make privacy choices and exercise relevant consumer data rights.[18] The Kids Seal Requirements integrate the General Seal's core privacy protections and add COPPA's provisions, insights from FTC and state enforcement actions, FTC guidance, and principles from state children's privacy law. The latest Kids Seal Requirements contain several "beyond COPPA" provisions that generally track state privacy laws like the Vermont AADC and provide substantive protections (e.g., high privacy defaults and "special care" to avoid a "heightened risk" of harm to children). There are similar provisions in the teen safeguard section of the General Seal Requirements.

For over three decades, the ESRB has been assigning age and content ratings to video games, and awareness and use among parents are consistently high.[19] Today, ESRB ratings also include upfront notices about interactive elements to ensure that parents are informed about features like player-to-player communications ("Users Interact") or the ability to spend money on virtual items ("In-Game Purchases") in games they may be considering for their families.[20]

Vermont families benefit from a variety of safety controls that ESA member companies have developed, such as filtering by age rating; limiting the visibility of personal information; managing the time or money kids can spend playing video games; and restricting, blocking, or reporting player-to-player communications (including customized options for muting certain words). ESRB further provides a centralized place with step-by-step parental control guides for consoles, Windows computers, and other platforms.[21] Companies also promote "positive play" so that players enjoy a game experience based on sportsmanship, camaraderie, and mutual respect, such as through codes of conduct and mechanisms to encourage positive values (e.g., incentive systems for positive behaviors, penalties for offensive chats, or warning systems to address disruptive players).[22] ESA members enhance their safety protocols by integrating

[18] *Privacy Certified Seals*, Ent. Software Rating Bd., https://www.esrb.org/privacy-certified-seals.

[19] Patricia E. Vance, *Research: No News is Good News When It Comes to Appropriate Video Games*, Ent. Software Rating Bd. (Nov. 11 2025), https://www.esrb.org/blog/research-no-news-is-good-news-when-it-comes-to-appropriate-video-games.

[20] *Ratings Guide*, https://www.esrb.org/ratings-guide

[21] *Tools for Parents*, Ent. Software Rating Bd., https://www.esrb.org/tools-for-parents/parental-controls/

[22] *Trust and Safety: Setting guidelines for acceptable online behavior*, Ent. Software Ass'n, https://www.theesa.com/trust-safety/codes-of-conduct.

research, new design approaches, and insights from players.[23] And ESA and its members partner with organizations to facilitate information sharing and coordination.[24]

Parents highly value the video game industry's privacy and safety resources, as reflected in our 2026 industry report. For example, nearly 80% of parents say they check the age rating "every time" or "most of the time" when buying or downloading a new game for their children.[25] And nearly 80% of parents use parental controls on a video game device.[26] More than two-thirds of parents say ESRB ratings and content descriptors help them to better understand what their kids see when playing video games compared to social media.[27] These findings affirm that existing practices in the video game industry help children and families to have safe and rewarding experiences playing video games.

III. Flexible and proportionate age assurance requirements will make young Vermonters safer and help them to enjoy positive online experiences.

In our experience, as expressed in our March comments, it is important for online safety regulations to be flexible and proportionate and to help parents decide what is right for their families. The proposed rules for age assurance could be strengthened by implementing these principles further. Specifically, we recommend removing the age assurance mandate, which is unauthorized under the AADC, and adjusting the purpose limit and deletion requirements for age data. These changes would help to make young Vermonters safer and broaden access to positive online experiences.

We applaud the AGO's efforts to take a flexible and proportionate approach to age assurance because this type of approach is essential to maintaining children's online privacy and safety. For example, requests for age information, beyond self-declaration, can be privacy-invasive and often result in a company collecting or sharing more information than otherwise needed to provide a product or service. Given the risk of data breaches and the sensitivity of information involved, the level of age assurance and information collected should be proportionate to the risk to the user associated with the activity or when needed to provide the service (e.g., for certain data processing activities). Moreover, regulations that are overly

---

[23] Some companies use artificial intelligence to detect cheating or help with blocking chats that violate codes of conduct (e.g., hate speech, discriminatory language, or harassment). Companies are also using image-hashing technology and machine learning to look out for harms like child exploitation. *Artificial Intelligence*, Ent. Software Ass'n, https://www.theesa.com/issues/ai.

[24] These organizations include groups like the National Center for Missing & Exploited Children, Family Online Safety Institute, Games for Change, Raising Good Gamers, Safer Internet Day, and Fair Play Alliance *Protecting players by working together*, Ent. Software Ass'n, https://www.theesa.com/trust-safety/working-in-partnership.

[25] ESA, 2026: Essential Facts About the U.S. Video Game Industry, https://www.theesa.com/wp-content/uploads/2026/06/2026-Essential-Facts-Booklet-05-27-26.pdf.

[26] *Id.*

[27] *Id.*

prescriptive run the risk of undermining online safety. For example, safety measures are most effective when requirements account for user behavior and buy-in. If users experience too much friction from new requirements, they may begin to utilize services or technology in unintended ways (e.g., users might use VPNs to avoid age assurance, or parents could share accounts to avoid hassle).

Given that the AADC does not authorize mandatory age assurance, and in light of the importance of proportionality, the AGO's rules should remove the age assurance mandate and allow covered businesses to pursue age assurance among their arsenal of other safety measures.[28] The AADC's rulemaking delegation is to "identify[] commercially reasonable and technically feasible methods" for age assurance, not mandate deployment.[29] Notably, the AADC expressly does not require age assurance for all such services, products, or features. Instead, it defines a "[c]overed minor" based on actual knowledge of the user's age or having used "age assurance methods."[30] Additionally, video game companies in particular often have legitimate reasons to not conduct age assurance. For example, a particular user experience may be premised on treating all users as minors. Overbroad requirements to conduct age assurance would result in the unnecessary collection of personal information.

We also recommend clarifying that a covered business has flexibility to use the output of age assurance for certain purposes beyond age assurance. The proposed rules limit the use of age assurance data to age assurance purposes, which could create confusion about whether this data can be used for certain other legitimate purposes, such as implementing safety defaults.[31] A covered business should have reasonable flexibility to use age assurance data for other safety and security purposes, eliminating the need to collect this age information multiple times. A repetitive collection process would result in the unnecessary collection of additional personal information from players, undermining privacy, and would also result in user frustration and friction, further undermining the age assurance process and safety. We therefore suggest that the rules clarify that age assurance data can be used for other purposes where appropriate consent is obtained and the underlying, raw personal information is appropriately deleted.

Additionally, the AGO should revise the proposed data deletion requirements to resolve a conflict with FTC guidance and reflect technical limits on data deletion, which will support efficiency and consistent compliance to better protect Vermonters. The proposed rules would

---

[28] *See* Proposed Rule for Section CP _ Applicability (c), Vt. Att't Gen., https://ago.vermont.gov/sites/ago/files/2026-07/AADC%20rules/2026.07.08%20-%202449g%20Age%20Assurance%20Privacy%20-%20FINAL%20DRAFT.pdf ("A covered business shall implement proportionate age assurance measures for any online service, product, or feature reasonably likely to be accessed by covered minors.").

[29] 9 V.S.A. § 2449g(b).

[30] *Id.* § 2449a(12).

[31] *See* Proposed Rule for Section 2449g at CP _ Prohibited Uses, Retention, and Disclosure of Age Assurance Data (a)-(b), Vt. Att't Gen., https://ago.vermont.gov/sites/ago/files/2026-07/AADC%20rules/2026.07.08%20-%202449g%20Age%20Assurance%20Privacy%20-%20FINAL%20DRAFT.pdf.

require deleting age information "immediately,"[32] but the FTC has established a different, more flexible approach, conditioning enforcement policies on an instruction not to retain information "longer than the period necessary to fulfill the Age Verification Purposes" and to "delete[] such information promptly thereafter."[33] The FTC's approach on this point is sensible because "immediate" deletion may not always be possible or serve the safety of users. For example, it can be technically challenging to delete information "immediately" at scale without introducing the risk of errors. Maintaining information for at least a brief period of time may also be necessary to allow for an efficient process if a user quickly appeals or seeks to redo the process. Indeed, in some circumstances, it could create user friction if the underlying basis for an age determination is not at least briefly maintained, undermining safety measures. As also noted, in some circumstances, a covered business may legitimately need to collect age information for multiple purposes. An alternative standard could require deleting age information within a "reasonable" period of time (and only if the information was collected solely for the purpose of age assurance), which would promote more consistent compliance and better safety outcomes by establishing standards that are achievable and allow for legitimate safety operations. These adjustments will make data more secure and Vermonters of all ages safer, particularly children.

IV. Flexible and proportionate requirements for data and design practices are also important to help young Vermonters have safe and positive online experiences.

We also believe that the proposed rules regarding data and design practices could be strengthened by emphasizing flexibility and proportionality, as well as doing more to help parents decide what is best for their families. We suggest adjusting the restrictions on monitoring and notifications to reduce the risk of inhibiting basic game functions, and we also suggest clarifying that the rules may not be interpreted to regulate content or other expressive activity. These changes would help to make young Vermonters safer and promote access to positive online experiences.

As drafted, the restrictions on "monitoring" are overbroad, resulting in unintended consequences. Under the rules, whenever a covered business engages in "monitoring," the covered business must provide a conspicuous signal to the user.[34] "Monitoring" is defined in part as "observing, collecting, recording, analyzing, or processing a covered minor's activity, behavior, or interactions with an online service, product, or feature."[35] The definition applies

[32] *Id.* at CP _ Data Minimization in Age Assurance (d), https://ago.vermont.gov/sites/ago/files/2026-07/AADC%20rules/2026.07.08%20-%202449g%20Age%20Assurance%20Privacy%20-%20FINAL%20DRAFT.pdf.

[33] FTC, Enforcement Policy Statement Promoting the Adoption of Age-Verification Technology (Feb. 25, 2026), https://www.ftc.gov/legal-library/browse/enforcement-policy-statement-promoting-adoption-age-verification-technology.

[34] See Proposed Rule for Section 2449f at CP _ Monitoring and Tracking (a), Vt. Att't Gen., https://ago.vermont.gov/sites/ago/files/2026-07/AADC%20rules/2026.07.08%20-%202449f%20Prohibited%20Data%20and%20Design%20Practices%20-%20FINAL%20DRAFT.pdf.

[35] *Id.* at CP _ Definitions (i).

regardless of "whether a covered minor's activity, behavioral data, or engagement data is linked to an identified or identifiable covered minor."[36] This broad structure could capture even service improvement activities that rely solely on anonymous data. Indeed, under this definition, simply loading a webpage to play a video game constitutes "monitoring" because the server records the page request. Consequently, a conspicuous signal would be needed essentially at all times, creating confusion, undermining the signal's informative value, and reducing safety.

We suggest a few changes to address this concern. At a minimum, the AGO could remove "[l]inked to an identified or identifiable covered minor" from the definition of "monitoring." Alternatively, an exception should be added to permit the collection and processing of truly anonymous data for activities that might otherwise fall within the scope of monitoring without requiring a conspicuous signal. Separately, because certain security-related activities (including fraud detection and anti-cheat technologies) could also fall within the "monitoring" definition, we would support an additional exception or carveout for these legitimate security-related use cases, allowing them to occur without triggering the conspicuous signal requirement.

Additionally, we suggest amending the proposed limits on notifications to allow for basic communicative and safety functions. The proposed rules would prohibit, at any time of day, "any notifications" or "notification features designed or reasonably likely to encourage, increase, prolong, or reinitiate a covered minor's engagement with an online service, product, or feature through the use of personal data, behavioral data, or inferred preferences."[37] This approach creates a problem because almost any notification could possibly be construed to be reasonably likely to "reinitiate" engagement, given that any notification will serve as a reminder of the existence of a service and provide information about the service. And, in turn, the phrase "through the use of personal data" captures essentially all useful notifications because nearly all useful notifications rely on personal data—they reference something specific to the child.

To help illustrate the issue, for example, an alert might communicate information about a message received from a friend on the platform or a security issue that needs to be addressed. Indeed, when parents affirmatively enable notifications for their children at certain hours, this could render the notifications conducted "through the use of personal data" (the child's schedule), overriding parental choice. Accordingly, ESA and its members are concerned that the rules would limit these basic communicative and safety functions. We therefore suggest narrowing the range of notifications covered under the rules, giving parents a clearer role in helping children to manage notifications, and providing clear exceptions from the rules for basic communicative and safety functions that do not primarily operate to pull a user back on a service.

The final regulations should also support creativity and free expression, as discussed in our March comments. Video games allow users to explore other worlds and be awed by epic

[36] *Id.*

[37] *Id.* at CP _ Engagement-Based Notifications (a).

stories. The First Amendment protects the speech rights of video game players and developers. The Supreme Court has explained that video games are expressive works, much like newspapers, books, movies, or music in this respect.[38] As the Supreme Court noted, video games "communicate ideas—and even social messages—through many familiar literary devices (such as characters, dialogue, plot, and music) and through features distinctive to the medium (such as the player's interaction with the virtual world)."[39] The rules should avoid a chilling effect on content and expressive activity.

Conclusion

In sum, Vermonters of all ages enjoy video games and benefit from the video game industry's leading privacy and online safety measures. Regulations that are flexible, proportionate, and empower parents will help to keep young Vermonters safe online. ESA welcomes the opportunity to discuss these views and our experience with the Attorney General.

Respectfully submitted,

Michael G. Lewis
Vice President & Associate General Counsel

[38] *Brown v. Ent. Merchants Ass'n*, 564 U.S. 786, 790 (2011).

[39] *Id.*

Bambara, Anthony

Subject: Vermont AADC Rulemaking Submission - Electronic Privacy Information Center (EPIC)

From: Megan Iorio <iorio@epic.org>
Sent: Friday, October 2, 2026 6:13 PM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Cc: Tom McBrien <mcbrien@epic.org>; Hayden Davis <davis@epic.org>
Subject: Vermont AADC Rulemaking Submission - Electronic Privacy Information Center (EPIC)

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Good afternoon,

Please find attached comments from the Electronic Privacy Information Center (EPIC) on the Attorney General's proposed rules for Sections 2249f and 2449g of the Vermont Age-Appropriate Design Code. Feel free to reach out to us at iorio@epic.org for further discussion.

All the best,

Megan Iorio
Senior Counsel
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, D.C. 20036
(202) 483-1140 x124
iorio@epic.org

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

VERMONT ATTORNEY GENERAL'S OFFICE

Re: Proposed Vermont Age-Appropriate Design Code Rules for

Sections 2449f of Act 63

October 2, 2026

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Vermont Attorney General's Office's ("AGO") proposed Prohibited Data and Design Protection Rule ("Proposed Rule") for the Vermont Age-Appropriate Design Code ("AADC"), to be codified in Section 2449f.[1]

EPIC is an independent, nonpartisan public interest research center in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. For decades, EPIC has worked under different administrations to safeguard individuals' personal data and to protect consumer privacy. Recently, EPIC has been a leading voice on platform governance issues, advocating for meaningful regulation and oversight of platform companies that respects the privacy, speech rights, and associational rights of platform users.

The Vermont AADC relies on effective and sustained Attorney General rulemaking for its efficacy. EPIC is grateful to the Attorney General for proposing such a detailed and

[1] Vermont Attorney General's Office, *Age Vermont Age-Appropriate Design Code Rulemaking* (July 8, 2026), https://ago.vermont.gov/vermont-age-appropriate-design-code-rulemaking.

thoughtful set of rules, and is glad to see the AGO recognize some of the most harmful design practices as worthy of prohibition. However, EPIC believes that a number of changes are still necessary. Most importantly, EPIC recommends that the AGO simplify the Proposed Rule to avoid statutory conflicts and unintended results, especially by removing some of the provisions not focused on prohibited practices. EPIC also offers a number of suggestions to more clearly define the prohibited practices identified in the Proposed Rule, which EPIC believes will help promote compliance and prevent litigation.

I. The AGO should simplify the Proposed Rule and focus its scope on prohibited practices to avoid statutory conflicts.

Section 2449f of the AADC directs the Attorney General to adopt rules "prohibit[ing] data processing or design practices of a covered business that, in the opinion of the Attorney General, lead to compulsive use or subvert or impair user autonomy."[2] While most of the Proposed Rule responds to this directive, a number of sections go beyond this scope. While the AGO has authority to promulgate rules on these other topics, many are already adequately covered by the statutory text itself. Expanding on these through the Proposed Rule threatens to have undesirable effects and even to conflict with the statute. As a result, EPIC recommends simplifying the Rule to remove some of these sections and focus on the harmful data-processing and design practices that the AADC explicitly relies on the AGO for rulemaking on.

A. Amend the "Applicability" section to conform with statutory definitions.

As a preliminary matter, EPIC recommends that the AGO strike part (b) of the Applicability section of the Proposed Rule to prevent inconsistent definitions. As currently

[2] Sec. 1. 9 V.S.A. chapter 62, subchapter 6 §2449f(b).

drafted, part (a) of the Applicability section correctly and appropriately identifies that the Rule applies to covered businesses insofar as their products are used by a covered minor. However, part (b) creates unhelpful confusion by adding that the Rule's requirements and provisions apply "where a covered business knows or has reason to know that a user is a covered minor" and then defining such knowledge in a circular way.

The AADC already includes a knowledge requirement of its own. The statute limits its definition of "covered business" to those whose "online products, services, or features are reasonably likely to be accessed to a covered minor," and in turn defines a "covered minor" as a consumer who "a covered business actually knows is a minor or labels as a minor pursuant to [the age assurance rulemaking the AGO has undertaken pursuant to Section 2449g]." The Proposed Rule's articulation of a separate—if superficially similar—standard of applying where a covered business "knows or has reason to know that a user is a covered minor" creates needless confusion as to what role this latter test plays. For simplicity and clarity, the AGO should rely on the knowledge standards already included in the AADC's text.

Furthermore, the Proposed Rule's articulation of when this "knows or has reason to know" standard is satisfied creates further issues. The Proposed Rule states that a covered business "shall be deemed to have reason to know that a user is a covered minor" whenever "The online service, product, or feature is reasonably likely to be accessed by a covered minor." But reasonable likelihood of access by a covered minor is, itself, a prerequisite for a company to be considered a covered business in the first place, making this definition circular. Under the Proposed Rule's definition, a covered business *inherently* knows or has reason to know that a user is a covered minor. This does not make sense and seems to conflict with Section

2449a(12)'s requirement that a covered minor is only one that the company *actually* knows or has *labeled* as a minor.

For these reasons, EPIC recommends that the AGO strike part (b) from the Applicability section of the Proposed Rule entirely. Part (a), accompanied by the statutory definitions of covered business and covered minor, already adequately defines the scope of the AGO's regulations, and should be allowed to stand alone.

B. The AGO should remove a number of sections that do not address prohibited processing and design practices.

Several sections of the Proposed Rule (specifically those not addressing prohibited data-processing and design practices) either restate statutory text in ways that risk confusion or actually conflict with the statute. In some cases, we fear provisions of the Proposed Rule, by broadening the statutory language, could also unintentionally limit useful functions of covered business's products. As a result, EPIC recommends the following sections of the Proposed Rule be removed:

Remove the General Duty Section. The General Duty section essentially restates the duty of care already provided in Section 2449c of the statute. However, the duty asserted in the Proposed Rule uses the term "heightened risk of harm" rather than the categories used in the statute (emotional harm, compulsive use, and discrimination). To prevent two similar but distinct duties of care, EPIC recommends removing this general duty from the Proposed Rule.

Remove the Foreseeability Section. Accordingly, EPIC also recommends removing the section on foreseeability. While the minimum duty of care in Section 2449c of the statute hinges on whether the harms are "reasonably foreseeable," this is a concept well-defined in law and that

courts are well-positioned to adjudicate. EPIC fears that the Proposed Rule's discussion of foreseeability threatens to complicate, rather than simplify, this analysis.

Remove the Data Minimization Section. Similar to the general duty section, the Proposed Rule's data minimization provisions largely repeat the statutory language but with some inconsistencies, for instance adding a prohibition on the "use" of data. We also have concerns that in certain contexts, some of the prohibitions added by this section could reduce benign and even useful functionality in unintended ways. EPIC also has serious concerns with the definition of "necessary to provide a service," which seems to conflict with the statute itself and is missing important provisions (such as a carveout for complying with legal obligations). We would recommend avoiding defining this term, or relying on definitions from other data minimization statutes.

Remove the Secondary Use Section. In the same vein, the secondary use section of the Proposed Rule again do not perfectly align with the statute, missing, for instance, the exception for secondary uses to comply with the AADC itself. Furthermore, some of the more specific prohibitions the Proposed Rule adds could create issues in certain contexts, such as for chatbots, for which a ban on inferring any preferences without exception would presumably limit considerable functionality. For these reasons, we recommend the AGO leave the statutory text itself to govern.

Remove the Monitoring and Tracking Section. Section 2449f(a) of the statute requires a conspicuous signal be provided to a minor whenever an individual is monitoring/tracking the online activity or location of the covered minor. However, the Proposed Rule seems to broaden this signaling requirement to any time even the covered business itself is internally tracking the user's behavior. This could create a situation where it is harder for a covered minor to tell when

an individual is actually tracking their activity, if the tracking signal is constantly present due to the platform's own tracking activity.

Remove the Personalized Media Section. This section of the Proposed Rule largely rephrases the provisions of Section 2449(f)(a)(4), and as a result seem duplicative and present an unnecessary risk of inconsistency. Indeed, some of the definitions provided in the Proposed Rule seem to undercut the statute's exceptions and limit benign functionality. The requirement that an "express and unambiguous request" be specific and contemporaneous, for instance, would seem to exclude lists of accounts a user follows, or prior requests to see more or less content of a certain type. What's more, many types of feed personalization are beneficial.[3] For this reason, feed personalization should not be categorically prohibited. Indeed, the statutory text allows personalization when based on signals expressly provided by a covered minor. EPIC thus suggests removing this section from the Rule and relying instead on the plain statutory language.

Remove the Sections Discussing Compulsive Use and Impairment of Autonomy. Finally, EPIC suggests removing the provisions on "Compulsive Use" and "Impairment of Autonomy." As drafted, these sections seem inconsistent with the standard set by the statute. For instance, while the statute defines "compulsive use" as repetitive use that "materially disrupts" a major life activity such as sleeping, eating, or learning, the Proposed Rule deems a practice as causing compulsive use if it meets any of four conditions, including being "reasonably likely to increase" usage. This turns a harm standard into an engagement standard. Given that the Proposed Rule already separately identifies specific data-processing and design practices that are prohibited for causing these harms, these two additional sections articulating "compulsive use" and

[3] Alissa Cooper, et al., *Better Feeds: Algorithms That Put People First*, Knight Georgetown Institute (March 2025), https://kgi.georgetown.edu/wp-content/uploads/2025/02/Better-Feeds_-Algorithms-That-Put-People-First.pdf.

"impairment of autonomy" more generally can be removed without undermining the Rule's efficacy. Doing so would simplify the Rule and prevent confusion.

In addition to removing the above sections themselves, EPIC recommends that the AGO remove definitions in the Proposed Rule made necessary by these sections. In particular, we have concerns about the definitions of "Select, recommend, or prioritize media," "Necessary to provide a service," and "Express and unambiguous request," which we fear are likely to cause confusion and statutory conflict.

A version of the Proposed Rule that eliminates these redundant or conflicting provisions, and focuses instead on prohibited data-processing and design practices, will be simpler to follow, better placed to withstand legal challenge, and more effective at protecting Vermont's youth.

II. The AGO should modify its description of certain prohibited practices for clarity.

The AGO's Proposed Rule identifies nine practices as prohibited for minors in accordance with Section 2449f(b) of the AADC. EPIC agrees with the AGO's determination that these practices lead to compulsive use or impair user autonomy and should be prohibited for minors. However, EPIC proposes the following revisions to more precisely define these practices and to avoid repetition. These changes do not significantly change the substance of the Proposed Rule, but rather serve to ensure that the prohibited practices are clearly and appropriately scoped, making it easier for covered businesses to comply and reducing the risk of litigation.

A. The AGO should expand the "Asymmetrical Interfaces" prohibition.

As currently drafted, the Proposed Rule only prohibits asymmetrical interfaces when they are designed to extend use. EPIC recommends expanding the definition to also prohibit asymmetrical interfaces that discourage covered minors from choosing more protective settings

more broadly. This broader definition is more in line with Section 2449f(b)'s directive to prohibit practices that "impair user autonomy," not just those that lead to compulsive use, and would prevent platforms from manipulating minors into turning off privacy protections.

Proposed Revisions:

> *(a) A covered business shall not design interfaces that make continued* ~~***engagement***~~ ***use, or a less protective setting,*** *substantially easier* ***for a covered minor to choose*** *than disengagement, exit, or reduction of use****, or a more protective setting*** ~~***by a covered minor***~~*.*
>
> *(b) Illustrative examples include, but are not limited to:*
>
> 1. *Hidden, obscured, or less accessible logout****,*** ~~***or***~~ *exit****, and privacy setting*** *controls;*
> 2. *Requiring additional steps, effort, or time to exit, disable features, or reduce use compared to continuing* ~~***engagement***~~ ***use****;* ~~***or***~~
> 3. *Interfaces that delay, discourage, or interfere with a covered minor's ability to disengage from the online service, product, or feature****; or***
> 4. ***Interfaces that make less protective settings more prominent than more protective settings****.*

In line with this, EPIC also recommends the AGO define "Less protective setting" as "a setting that decreases a user's privacy or safety protections, including but not limited to increasing the amount of personal data a covered business collects or processes about the user, decreasing the user's privacy with respect to other users, or increasing the risk of causing compulsive use."

B. The AGO should clarify the "Autoplay" prohibition.

Though somewhat intuitive, "autoplay" design practices can be hard to precisely define with sufficient specificity to avoid vagueness concerns. EPIC suggests building off the definition of autoplay used in the recent Meta settlement and suggest the following language accordingly.

Proposed Revisions:

> *(a) A covered business shall not automatically initiate* ***or resume playback of*** *media without* ***an affirmative and unambiguous*** *action by a covered minor.*
>
> *(b) Illustrative examples include, but are not limited to:*
>
> 1. *Automatic playback of videos* ***upon opening an online product, service, or feature****; or*
> 2. ~~***Auto-advancing media***~~ ***Automatic playback when a video becomes visible on a screen or when a covered minor hovers over a video****.*

C. The AGO should merge the prohibitions on "Behavioral Recommendation Systems," "Engagement-Based Notifications," and "Reinforcement Mechanisms" into a single prohibition on usage maximization systems.

The Proposed Rule currently contains separate prohibitions on engagement-optimizing "Behavioral Recommendation Systems," which use personal/behavioral data and inferences to prioritize content, on "Engagement-Based Notifications," which target notifications to maximize minors' engagement, and on "Reinforcement Mechanisms" that use variable/intermittent rewards to drive engagement from minors. All of these are examples of the broader design practice of engagement-maximization, or more accurately "usage-maximization." For simplicity, EPIC recommends merging these sections into a single prohibition on "Usage Maximization Systems," and providing usage-maximizing feeds, engagement-based notifications, and reinforcement mechanisms as illustrative examples. This change would streamline the rules while more directly addressing the underlying harm of these practices—that they manipulate minors into overuse.

Proposed Revisions:

> *(a) A covered business shall not* ~~***implement or deploy any system that***~~ *use*~~***s***~~ ***a covered minor's*** *personal data, behavioral data,* ***behavioral inferences,*** *or inferred preferences to* ~~***select, recommend, rank, order, prioritize, or sequence media for a covered minor***~~ ***extend, increase, optimize, or maximize user engagement, session time, or frequency of use****.*
>
> *(b)* ~~***Such systems rely on engagement optimization and operate without express and unambiguous request by a covered minor.***~~ ***A covered business shall not use variable***

reward schedules on a covered minor, regardless of whether such features use data about the minor.

(c) Illustrative examples include, but are not limited to:

1. *Algorithmic* ~~***feeds***~~ ***recommendation systems*** *that* ***use usage maximization techniques to select,*** *prioritize,* ~~***rank,***~~ *or recommend media* ~~***based on a covered minor's behavioral data, inferred preferences, or prior activity***~~*;*
2. ~~***"For You" feeds***~~ ***Using a variable reward schedule to distribute rewards or other incentives to a covered minor****;* ~~***or***~~
3. ~~***Engagement-ranked media***~~ ***A chatbot that uses a covered minor's interactions with the chatbot to manipulate the covered minor into extending their session or initiating a new session; or***
4. ***Using usage maximization techniques to the determine the timing, frequency, or batching of push notifications for a covered minor****.*

In line with this, EPIC also recommends amending the definition of "engagement optimization" to "usage maximization", and clarifying that it means "techniques used to ~~**increase**~~ **optimize** a covered minor's ~~**interaction**~~ **engagement with an online service, product, or feature**, session duration, or frequency **of use**."

D. The AGO should clarify some of the illustrative examples in the "Circumvention" prohibition.

EPIC recommends making the third illustrative example more concrete, to provide a clearer demonstration of what sort of conduct constitutes circumvention. As originally drafted, the third illustrative example largely echoed the language of the rule itself. Instead, we suggest moving the circumvention provision from the "Push Notification" section of the Proposed Rule into an illustrative example here, placing all of the circumvention prohibitions in one place and providing a clearer example of prohibited activity.

Proposed Revisions:

(a) A covered business shall not design, implement, modify, or deploy a feature, interface, or practice that:

1. *Achieves substantially similar effects as a prohibited practice through alternative design, technical, or operational means; or*

2. Circumvents or attempts to circumvent the intent, purpose, or requirements of this Rule.

(b) In determining whether a practice constitutes circumvention, the Attorney General may consider whether the practice:

1. Replicates or replaces engagement optimization effects through alternative mechanisms or design features;

2. Produces substantially similar effects on a covered minor's engagement, behavior, or decision-making as a prohibited practice;

3. Uses alternative signals, metrics, or behavioral indicators to achieve outcomes otherwise prohibited by this Rule; or

4. Replaces a prohibited feature with a substantially equivalent feature designed to achieve similar engagement outcomes.

(c) Illustrative examples include, but are not limited to:

1. Redesigning a prohibited feature while preserving substantially similar engagement effects;

2. Using alternative ~~***behavioral***~~ ***user*** *signals or* ~~***inferred preferences***~~ ***inferences*** *to optimize engagement;*

3. ~~***Replacing prohibited notifications, prompts, or recommendation features with substantially equivalent engagement mechanisms***~~ ***Substituting notifications with functionally equivalent prompts, alerts, or messages delivered through other means****; or*

4. Modifying the presentation, timing, or delivery of a prohibited practice while maintaining substantially similar behavioral effects.

E. The AGO should more precisely define "Continuous Media Feeds" to prevent ambiguity.

EPIC recommends changing the definition of "Continuous Media Feeds" to more precisely target the sort of "infinite scroll" features that lead to compulsive use. We believe this revised language is better placed to withstand a vagueness challenge from industry.

Proposed Revisions:

(a) A covered business shall not ~~***provide media streams that automatically load or***~~ *continuously* ~~***present***~~ *add****itional*** ~~***itional***~~ ***new*** *media* ***to an algorithmic feed seamlessly and*** *without requiring a****n*** ~~***discrete and intentional***~~ *action by a covered minor* ***to request such additional media****, beyond* ~~***ordinary***~~ *scrolling or* ~~***navigation***~~ ***swiping***~~***, to access such additional media***~~*.*

(b) Illustrative examples include, but are not limited to:

1. *Infinite scroll interfaces;*
2. *Interfaces that automatically* ***and continuously*** *load additional media* ***indefinitely*** *as a covered minor scrolls, swipes, or otherwise* ~~***engages in ordinary navigation***~~ ***navigates across a page****; or*
3. *Continuously* ~~***presented***~~ ***loading*** *media* ~~***streams without***~~ ***features that lack*** *a clear stopping point* ~~***or a***~~ ***wherein a covered minor is required to take an affirmative action to request*** ~~***discrete and intentional action by a covered minor, beyond ordinary scrolling or navigation, to access***~~ *additional media.*

F. The AGO should strengthen the "Push Notification" restrictions in line with the recent Meta Settlement.

Parts of the Proposed Rule's push notification restrictions, specifically sections (a), (b), (c), and (f), are most naturally covered by other sections of the Rule, specifically by the prohibitions on usage maximization systems, social pressure functions, and circumvention. As a result, to avoid duplication, EPIC suggests focusing this section instead on just three things: (1) limiting notifications to minors during nighttime; (2) limiting notifications to minors during school hours; and (3) ensuring minors have control over what types of notifications to receive at all other times.

Prohibiting Nighttime Notifications. The Proposed Rule already would prohibit nighttime notifications to minors between midnight and 6 a.m. EPIC suggests broadening this nighttime notification ban to 10 p.m. to 7 a.m. This is consistent with the nighttime notification ban included in the recent Meta Settlement, and would provide covered minors with a greater period of uninterrupted sleep.

Prohibiting School-Hour Notifications. In addition to nighttime notifications, the AGO should also prohibit notifications during school hours. This, too, was included in the Meta Settlement, which prohibits push notifications from 8 a.m. to 3 p.m. from August 15 through June 15 each year. The AGO should adopt a similar restriction calibrated to the dates of the

typical Vermont school year. Preventing notifications during school hours is vital for reducing distraction in schools and for discouraging minors from circumventing school phone bans.

Securing Control Over Notification Categories. Equally important, EPIC also recommends that the AGO revise the Proposed Rule to prohibit covered businesses from providing a single setting to turn all push notifications on during times in which such notifications are allowed. Section 2449d(a)(H) requires covered businesses to turn push notifications off for minors by default. However, it is likely that minors will opt to receive certain push notifications, such as notifications alerting them of a new direct message. It is important that, in doing so, minors be given control over what types of notifications they wish to receive, and which they would rather leave off, and that businesses not be allowed to force minors into a false "all-or-nothing" choice. A requirement that covered businesses that offer multiple categories of push notifications give minors control over each category, and not provide a single option to turn all notifications on, would give minor users more autonomy over their online experience and reduce the number of notifications received.

Prohibiting these three practices would bring the AGO's rule in line with the Meta Settlement, prevent the most harmful effects of push notifications for minors, and prevent this section of the Rule from duplicating the provisions already covered elsewhere.

Proposed Redraft:

> ~~***(a) A covered business shall not send push notifications to a covered minor designed or reasonably likely to encourage repeated, prolonged, or compulsive engagement.***~~
>
> ~~***(b) Prohibited notifications include any notification that:***~~
>
> > ~~***1. Is based on personal data, activity, or behavioral data;***~~
> >
> > ~~***2. Is triggered by predicted or inferred preferences, interests, or likelihood of engagement; or***~~
> >
> > ~~***3. Encourages a covered minor to return to, continue using, or increase use of an online service, product, or feature through the use of personal data, behavioral data, or inferred preferences.***~~

~~*(c) A covered business shall not:*~~

~~*1. Use a covered minor's personal data to determine the timing, frequency, or media of notifications for purposes of increasing engagement; or*~~

~~*2. Use a covered minor's behavioral data or inferred preferences to trigger or optimize notifications.*~~

~~*(d)*~~ *(a) A covered business shall not send any push notification to a covered minor between the hours of* ~~*12:00 a.m.*~~ ***10:00 p.m.*** *and* ~~*6:00 a.m.*~~ ***7:00 a.m.***~~*, except where necessary to provide a transactional, safety, or account-related notification requested by a covered minor*~~*.*

~~*(e)*~~ ***(b) A covered business shall not send any push notification to a covered minor between the hours of 8:00 a.m. and 3:00 p.m. on Monday through Friday each week between Labor Day and June 20 [NOTE: EPIC recommends calibrating these dates to the typical Vermont school schedule].*** ~~*This section shall not prohibit:*~~

~~*1. Notifications that are necessary to provide an online service, product, or feature in direct response to an express and unambiguous request by a covered minor;*~~

~~*2. Notifications that provide transactional, safety, or account-related information and are not designed to increase engagement; or*~~

~~*3. Notifications expressly requested by a covered minor.*~~

~~*(f)*~~ ***(c) A covered business that provides multiple categories of push notifications through an online product, service, or feature, such as notifications concerning direct messages, peer activity, software updates, and offers, shall provide consumers with settings to enable or disable each specific category of push notification offered by the covered business on the online product, service, or feature, and shall not provide a single setting that turns all categories of push notifications on.*** ~~*A covered business shall not circumvent this section by:*~~

~~*1. Modifying the format, timing, or delivery mechanism of a notification to achieve substantially similar engagement effects; or*~~

~~*2. Substituting notifications with functionally equivalent prompts, alerts, or messages delivered through other means.*~~

~~*(g) Examples of prohibited push notifications include, but are not limited to:*~~

~~*1. Notifications encouraging a covered minor to return to a service based on prior activity;*~~

~~*2. Alerts highlighting new or recommended media likely to increase engagement;*~~

~~*3. Reminders or prompts designed or reasonably likely to encourage continued use or repeated access;*~~

~~*4. Notifications triggered by a prediction that a covered minor is likely to re-engage.*~~

G. The AGO should make minor clarifying edits to the "Social Pressure Features" prohibition.

EPIC recommends some small tweaks to the prohibition on "Social Pressure Features" to clarify the scope of the prohibition.

Proposed Revisions:

> *(a) A covered business shall not implement features designed to create social pressure, urgency, or perceived obligation for a covered minor to engage with* ***or otherwise use*** *an online service, product, or feature.*
>
> *(b) Illustrative examples include, but are not limited to:*
>
> 1. *Streaks or other features that reward continuous or repeated engagement* ***or use****;*
> 2. *Missed activity alerts, inactivity notices, or reminders* ***to access an online service, product, or feature,*** *designed or reasonably likely to encourage a covered minor to return to the online service, product, or feature;*
> 3. *Peer activity* ~~***prompts***~~ ***alerts****, including notifications that friends, peers, or contacts are active, engaging, or waiting;*
> 4. *Popularity indicators, engagement counts, or social comparison features designed or reasonably likely to* ~~***encourage continued engagement***~~ ***increase engagement, usage, session length, or frequency of use****; or*
> 5. *Features that create a perceived social consequence for disengaging, delaying response, or failing to maintain* ~~***activity***~~ ***consistent use****.*

H. The AGO should remove the duplicative "Illustrative Applications" section at the end of the Proposed Rule.

The Proposed Rule currently includes illustrative examples for each of the prohibited design practices, as well as a standalone "Illustrative Applications" section at the end of the Proposed Rule listing three "examples of practices that may violate multiple provisions" of the Rule. EPIC believes that, given the examples provided throughout the Proposed Rule, that these three final illustrations are duplicative and would recommend they be removed for simplicity and concision.

***

We are grateful to the Attorney General for continuing to lead on keeping kids safe online, and thank you for considering our recommendations. Please contact the Director of EPIC's Platform Governance and Accountability program, Megan Iorio, at iorio@epic.org with any questions.

Sincerely,

/s/ Megan Iorio
Senior Counsel & Director of Platform Governance

/s/ Tom McBrien
Counsel

/s/ Hayden Davis
Law Fellow

ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

VERMONT ATTORNEY GENERAL'S OFFICE

Re: Proposed Vermont Age-Appropriate Design Code Rules for

Sections 2449g of Act 63

October 2, 2026

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Vermont Attorney General's Office's ("AGO") proposed Age Assurance Privacy Rule ("Proposed Rule") for the Vermont Age-Appropriate Design Code ("AADC"), to be codified in Sections 2449g.[1]

EPIC is an independent, nonpartisan public interest research center in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. For decades, EPIC has worked under different administrations to safeguard individuals' personal data and to protect consumer privacy. Recently, EPIC has been a leading voice on platform governance issues, advocating for meaningful regulation and oversight of platform companies that respects the privacy, speech rights, and associational rights of platform users.

EPIC offers the following principles to ensure age assurance is implemented in a way that minimizes speech and privacy concerns:

[1] Vermont Attorney General's Office, *Age Vermont Age-Appropriate Design Code Rulemaking* (July 8, 2026), https://ago.vermont.gov/vermont-age-appropriate-design-code-rulemaking.

- Tailor age assurance to the harm by age gating harmful data and design practices, not entire online services and products.
- Make age assurance proportionate to the harm and sensitive to impacts on accessibility and usability.
- Minimize data collection by requiring operators to use information they currently possess before requesting additional personal data.
- Include strong privacy protections for any personal data collected for age assurance.
- Provide consumers with choice of age assurance methods.
- Provide an effective and responsive appeals process.
- Provide the public with transparency about age determination practices.

To that end, EPIC recommends that the AGO:

- Remove the proportionality framework and instead make relevant determinations about proportionality.
- Remove language that would require all covered businesses to assess every consumer's age.
- Revise the graduated escalation framework to accurately capture privacy interests.
- Ensure all consumers, and all personal data, receive protections under the Rule, not just covered minors.
- Determine which businesses can provide consumers with multiple options for age assurance within commercial reasonability.
- Clarify the appeals process.
- Require public transparency into age assurance systems.

I. The applicability of the Proposed Rule should be based on whether a covered business engages in regulated practices and should not require all covered businesses to determine every consumer's age.

Age assurance requirements, when implemented correctly, can help ensure that businesses do not subject minors to harmful data and design practices. But age assurance must be implemented in way that is proportionate to the harm of the regulated practice, the protections provided by the statute, and the impact on privacy and accessibility. These proportionality decisions must not be left to the covered businesses to make—the AGO must make these decisions for the businesses.

The VTAADC classifies regulated practices into a risk framework, and the AGO should use this risk framework to define a proportionate age assurance framework. Practices that are prohibited for covered minors—ones that are listed in the high-risk practices section, prohibited by the duty of care, or described by the AGO's proposed rules on prohibited data and design practices—represent the highest risk category and covered businesses should not be able to subject consumers to those practices without first determining that they are not covered minors. The default settings requirements identify lower risk practices that minors can turn on and off. The AGO should not require covered businesses to collect additional data from consumers to determine whether they are covered minors to comply with these requirements.

EPIC thus recommends that the AGO:

A. Remove all references to proportionate age assurance.

The AGO should not allow covered businesses to decide what age assurance is proportionate. The VTAADC has already made many of these decisions, and the AGO should make the rest. Leaving these decisions to covered businesses will result in disjointed and confused compliance, including businesses that over-comply by age gating their entire services,

and businesses that under-comply by failing to use appropriate means to determine that a consumer is not a minor before subjecting them to harmful data and design practices.

The framework that the AGO outlines in the Age Assurance Selection section is an appropriate framework for the AGO to use to determine the rules regarding age assurance, but the AGO should not give covered businesses discretion to make these determinations. EPIC illustrates below how the AGO should use this framework to announce a more concrete Rule:

Foreseeability of harm. The VTAADC has already determined the foreseeability of harm for regulated practices. The VTAADC provides two categories of protections: It prohibits certain practices because they carry a high risk of harm and it sets default settings covered minors can change when there is a lower risk of harm and/or countervailing benefits of a practice. No consumer should be subjected to the data and design practices prohibited by the VTAADC unless the covered business first determines the consumer's age range under the Proposed Rule. A lower standard of age assurance would be appropriate for the default privacy settings provisions if additional factors, like privacy and accessibility, would be negatively impacted by using the same standard as the prohibited practices.

Accessibility and functionality. Age assurance should not be a barrier to accessing an entire online product or service. The VTAADC prohibits data and design practices that are simply not necessary for the functionality of any online product or service and thus could be turned off by default—or eliminated entirely—for all consumers. To preserve user accessibility and functionality, any covered business that wishes to offer any prohibited practice or feature should **only age gate the prohibited practice or feature** and not their entire product or service. Most of the default privacy settings and tools could also be implemented as defaults for all to ensure that age assurance does not become a barrier to accessing entire online products or

services. The one exception is the set of settings concerning features that connect covered minors and known adult users, as a covered business would need to know which group a consumer belonged to prior to providing online products and services that facilitate communication between users. To prevent the minor-adult default settings from being a barrier to accessing entire communications products and services, the AGO should allow covered businesses to rely on data they have previously collected about a user to determine whether they are a covered minor for the purposes of complying with the default privacy settings and tools provisions.

Privacy. Covered businesses should be encouraged to use information they already have to assess age, subject to certain conditions, before requesting additional data from consumers. If a covered business must collect additional data, the business should be required to use privacy-preserving technology, like zero-knowledge proofs and on-device processing, when technically feasible. The AGO's proposed Graduated Escalation provision can be modified to capture these requirements.

Accuracy. All covered businesses that subject consumers to prohibited practices should adhere to the same accuracy standards, and the AGO should announce these standards in the final Rule.

B. Make the rule apply to any covered business that engages in regulated practices.

In the Applicability section, provision (b) states that "This Rule applies where a covered business knows or reasonably should know that a user is a covered minor." But all covered businesses should be subject to the rule if they engage in any practice regulated by the VTAADC. The AGO should strike (b) and replace with "This Rule applies to any covered business that has obligations under 9 V.S.A §§ 2449c, 2449d, 2449f, or 2449g."

C. Do not require all covered businesses to determine whether a consumer is a covered minor.

In the Applicability section, provisions (c) and (d) state:

> *(c) A covered business shall implement proportionate age assurance measures for any online service, product, or feature reasonably likely to be accessed by covered minors.*
>
> *(d) A covered business shall determine whether a user is a covered minor using a proportionate age assurance method.*

The AGO should strike these two provisions. These provisions seem to require that all covered businesses determine the age of every consumer who accesses their online product or service. Such an expansive age determination mandate is neither necessary nor proportional to the risk of harm. Not all covered businesses engage in practices regulated by the VTAADC. Those businesses should not be required to assess any consumer's age. As for covered businesses that do engage in regulated practices, age assurance should **only be performed prior to subjecting a consumer to a feature or practice that is prohibited for covered minors and should never be mandatory**—all consumers must be able to default into the protections afforded by the VTAADC instead of having their age range determined.

D. Require covered businesses assure age only when a consumer requests a high-risk practice.

To clarify the scope of the Proposed Rule along the lines suggested above, the AGO should add the following provision to the Applicability section:

> *(c) A covered business shall determine whether a consumer is a covered minor according to this Rule when a consumer requests a practice prohibited for covered minors under 9 V.S.A §§ 2449c or 2449f, including any applicable rules.*

E. To comply with the default privacy settings requirements, covered businesses should be required to use existing data on consumers, not collect additional data.

To prevent age assurance from acting as a barrier to accessing entire online products and services, and taking into consideration the lower risks and protections encompassed in the default privacy settings and tools provisions, the AGO should add the following provision to the Applicability section:

> *(d) A covered business shall determine whether a consumer is a covered minor according to this Rule if it has obligations under 9 V.S.A § 2449d, including any applicable rules, but shall not be required to collect any personal data to determine age range for the sole purpose of complying with the section.*

II. The graduated escalation framework should be modified to accurately reflect data minimization principles.

The Graduated Escalation section of the Proposed Rule could be a useful framework for covered businesses to use to design their age assurance systems, but the Proposed Rule does not accurately capture the relative invasiveness of various age assurance methods.

The privacy implications of an age assurance method depend on the extent to which the method:

- Requires a covered business or processor to collect or process any personal information beyond what the covered business already collects or processes;
- Requires a covered business or processor to collect or process sensitive personal information, such as biometric data or government identification documents;
- Creates a risk of linkability between a consumer's identity and their online activities;

- Presents a risk of contributing to or entrenching commercial surveillance through secondary use, such as through data sale or use for targeting advertising; and
- Increases the risk that personal data is exposed through a data breach.

The VTAADC's primary method of mitigating privacy concerns is through its statutory privacy protections, along with the additional privacy protections contained in the Proposed Rules. By choosing an age assurance method that meets these privacy requirements, a covered business will minimize data collection and processing as well as linkability, secondary use, and data security risks.

When it comes to choice of age assurance method, the relative privacy invasiveness is not as simple as whether the method involves collecting or processing a particular age signal. For example, a credential-based method could be more privacy protective than a method that analyzes a consumer's behavior on a platform if the credential-based method processes all personal data on the consumer's device and transmits an age signal using a zero-knowledge proof. That is because, with on-device processing, the covered business never collects the consumer's personal data, and with the zero-knowledge proof, the covered business does not learn the consumer's identity, and the processor does not learn anything about the consumer's online activity. An age assurance method that relies on behavioral profiling could potentially involve the covered business processing large amounts of personal data and even collecting behavioral data that is otherwise not necessary to provide the online service, product, or feature to the consumer. There is, however, a reason to prohibit covered businesses from *solely* determining age based on credential-based age assurance: not every consumer has the required credentials to prove age. Thus, the AGO should require that covered businesses that use credential-based age assurance offer some alternative means of assessing age.

The AGO should modify the Graduated Escalation provision to accurately capture data minimization principles by directing covered businesses to first use data they may currently possess that is highly likely to be correlated with age.[2] The rule should be specific as to which signals are acceptable and when they are sufficient to satisfy the age determination requirement. For instance, self declaration that a consumer is a minor is highly likely to mean that the consumer is a minor, as users only have an incentive to falsely declare that they are adults to avoid platform access controls. Meanwhile, the AGO could declare that a consumer who created their account over ten years ago is sufficiently likely to be over the age of 18 that the consumer need not undergo any additional age assurance.

Once covered businesses have exhausted their existing age signal data, they should then be directed to use privacy-preserving means of processing and transmitting age signals to the extent that such privacy-preserving technology is commercially reasonable and technically feasible. Under the VTAADC, the AGO must be the one to determine that a privacy-preserving technology meets this standard, either by declaring that the technology is commercially reasonable and technically feasible, or by defining a clear market condition that, when met, would mean that the technology must be adopted.[3]

EPIC suggests the following language to replace provisions (a) and (b) in the Graduated Escalation section of the Proposed Rule:

> *(a) To minimize the collection and processing of personal data for age assurance, a covered business shall first use age signals currently in its possession to*

[2] 9 V.S.A § 2449g(b)(2)(B)(v)(I) (directing the AGO to consider "the efficacy of requiring covered businesses and process to use previously collected data to determine user age.")

[3] 9 V.S.A § 2449g(b)(1) (the AGO "shall . . . adopt rules identifying commercially reasonable and technically feasible methods for covered businesses and processors to determine if a user is a covered minor . . . .")

determine age range, if possible, and then use minimally invasive methods that employ privacy-preserving technology. This shall include:

1. *Self Declaration. Self declaration that a consumer is a minor shall constitute actual knowledge that the consumer is a covered minor. Self declaration that a consumer is not a minor shall not be sufficient to support a determination that a consumer is not a covered minor.*
2. *Account Age. Any consumer that opened their account over 10 years prior to the date of assessment shall not be considered a covered minor.*
3. *Existing age determinations or inferences. The covered business shall use any determinations or inferences of the consumer's age or age range, or any inferences correlated with age or age range, that the covered business has associated with the consumer, including any inferences the business has used to target advertisements to the consumer, to assign a consumer an age range.*
4. *Privacy-preserving technology. If a covered business must collect additional data from a consumer to determine their age range, the business shall use privacy-protective techniques, such as zero-knowledge proofs and on-device processing of personal data, [as far as the AGO has determined is commercially reasonable and technically feasible.]*

(b) If a covered business is not able to determine a consumer's age range using one of the methods described in (a), the business may use other methods of determining whether a consumer is or is not a covered minor that conform to the standards established in 9 V.S.A § 2449g and this Rule, provided that:

1. *If the covered business intends to process personal data it has previously collected about a consumer to determine age range, other than through the methods described in (a), the business must first request the consumer's separate and affirmative consent for the processing and provide the consumer a prominent and accessible means to opt out of the processing on an ongoing basis following consent.*
2. *A covered business shall not solely offer consumers the option of credential-based age assurance.*

EPIC also suggests the following change to provision (d) to conform to the above changes:

> *(d) Prior to selecting a**n** ~~moderate-intrusion or higher-intrusion~~ age assurance process or technique, a covered business shall:*
>
> *1. Evaluate ~~at least one lower-intrusion alternative~~ **all methods described in (a)**;*
>
> *2. Document ~~why such alternative is not reasonably available or sufficient to achieve the reasonably necessary level of accuracy or confidence~~ **whether and to what extent such methods could be used to determine consumers' age ranges, including the percentage of consumers whose age ranges could be determined using each method**; and*
>
> *3. Document the basis for selecting ~~the~~ **each** age assurance process or technique used.*

III. Protections should apply to all consumers, not just covered minors, and should clearly protect all personal data.

Several sections of the Proposed Rule describe privacy and accessibility protections but only afford those protections to "covered minors." All of the provisions in these sections should

replace "covered minor" with "consumer" where appropriate to ensure that all consumers are afforded the same rights:

- Frequency and Reassessment
- Data Minimization in Age Assurance
- Linkability and System Design
- Prohibited Uses, Retention, and Disclosure of Age Assurance Data
- Fallback and Accessibility
- Appeals Process

The Proposed Rule also uses imprecise language in numerous places to describe personal data. All instances of "age assurance data" should be revised to "personal data collected for age assurance purposes." Wherever the rule mentions "raw personal data", the term "raw" should be struck.

IV. Assess the commercial reasonability of large businesses providing consumers with multiple options for assessing age.

The AGO should determine whether it is commercially reasonable for the Rule to require covered businesses with a certain amount of annual revenue provide consumers with multiple age assurance options.[4] User choice will aid consumer adoption of age assurance methods. Not all consumers will be comfortable with the same age determination methods. Some consumers may be comfortable submitting to a face scan, while others may not. Real or perceived biases in age determination methods may also influence which methods consumers are willing to use and which ones are likely to give the consumer an accurate determination. The largest covered

[4] 9 V.S.A § 2449g(b)(2)(B)(v)(III) (directing the AGO to determine "the efficacy of requiring covered businesses and processors to provide users with multiple options for age assurance.")

businesses are likely to be able to provide consumers with multiple options for age assurance method and the AGO should require them to do so.

V. Prohibit covered businesses from limiting their appeals processes to a show of ID and clarify other aspects of the appeals process.

The AGO should add one condition and two clarifications to the Appeals Process section. First, covered businesses' appeals processes should not be based solely on credential-based age assurance for the same reason that their primary age assurance system should not rely solely on credentials: not all consumers have the appropriate documents to demonstrate age. Second, the Rule should make clear that the appeals process must adhere to all of the requirements in the Rule for age assurance generally as well as the VTAADC's statutory requirements. Finally, EPIC recommends that the AGO set a timeline for when covered businesses must respond to appeals, otherwise businesses may not properly staff the appeals process and consumers may experience extensive delays.

VI. Require covered businesses to make publicly available reports on their age assurance systems.

EPIC lauds the AGO for including strong assessment and documentation requirements in the Proposed Rule. Covered businesses should, however, be required to make a report based on this documentation publicly available on an annual basis. A public report will aid researchers in assessing covered business's age assurance systems, resulting in information that will help the AGO refine this Rule in the future. A public report will also provide consumers with much-needed transparency into how their data is collected, processed, and secured for age assurance purposes.[5] A covered business should be required to publish this report in a prominent and

[5] 9 V.S.A § 2449g(b)(2)(B)(iv) (directing the AGO to consider "whether and to what extent transparency measures would increase consumer trust in an age assurance method.")

accessible location on its website and also link to the report whenever it requests that a consumer undergo an age assurance process.

VII. Conclusion

EPIC commends the AGO on the Proposed Rules and is eager to engage with the AGO further regarding this rulemaking. Please contact the Director of EPIC's Platform Governance and Accountability program, Megan Iorio, at iorio@epic.org with any questions.

Sincerely,

/s/ Megan Iorio
Senior Counsel & Director of Platform Governance

/s/ Tom McBrien
Counsel

/s/ Hayden Davis
Law Fellow

ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)

Bambara, Anthony

Subject: Common Sense Media Comments in Response to Vermont Age-Appropriate Design Code Rulemaking

From: Lauren Jackson <ljackson@commonsense.org>
Sent: Friday, October 2, 2026 4:42 PM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Cc: Holly Grosshans <hgrosshans@commonsense.org>; Amina Fazlullah <afazlullah@commonsense.org>; Ariel Fox Johnson <afoxjohnson@commonsense.org>; Brenna Leasor <bleasor@commonsense.org>
Subject: Common Sense Media Comments in Response to Vermont Age-Appropriate Design Code Rulemaking

Some people who received this message don't often get email from ljackson@commonsense.org. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Hello,

Attached are Common Sense Media's Comments in Response to Vermont Age-Appropriate Design Code (AADC) Rulemaking. You can also view them here: https://www.commonsensemedia.org/sites/default/files/featured-content/files/common-sense-media-comments-in-response-to-the-vermont-attorney-general-s-office-ago-solicitation-of-comments.pdf

Please let me know if anything else is required on our end to submit, and thank you for the opportunity to comment.

Best,
Lauren Jackson
--
Lauren
Jackson
Advocacy
Project Coordinator
610.470.5541

common sense media



Comments in Response to the Vermont Attorney General's Office Solicitation of Public Comment Regarding Implementation of the Vermont Age-Appropriate Design Code

Respectfully submitted,

Holly Grosshans, Senior Counsel for Tech Policy
Common Sense Media

October 2, 2026

Common Sense Media's Comments in Response to the Vermont Attorney General's Office Solicitation of Public Comment Regarding Implementation of the Vermont Age-Appropriate Design Code.

Introduction.

Common Sense Media is the leading non-profit organization dedicated to protecting and preparing children, teens, and their families in the digital and AI world. Our mission is to improve the lives of children and families by providing the trustworthy information, education, and independent voice they need to thrive. Our ratings, research, and resources reach more than 150 million users worldwide, over 1.5 million educators, and more than 100,000 schools worldwide every year. Backed by the research that forms the foundation of everything we do, we champion quality media that entertains and inspires, and support legislation and regulations aimed at closing the digital divide and holding social media and AI platforms accountable for their effects on minors. We encourage students and educators to think critically about technology and become responsible digital citizens. And we help safeguard children's health and well-being by supporting the protection of their data privacy and reducing potential online harms.

Common Sense Media is pleased to submit these comments in response to the Vermont Attorney General's Office's (AGO's) request for public comment and feedback regarding implementation of the Vermont Age-Appropriate Design Code (AADC). As a trusted global organization dedicated to improving the lives of children and families, Common Sense welcomes the opportunity to bring our experience and perspective to this important rulemaking process. We strongly support the AGO's efforts to protect children's safety, privacy, and well-being online and offer the following recommendations to help ensure that the regulations provide meaningful, practical protections for Vermont's children and teens.

Risks Abound for Kids Online.

Children and teens spend a substantial amount of time online, and social media has become a significant part of their daily lives. According to the U.S. Surgeon General's 2023 advisory, Social Media and Youth Mental Health, up to 95% of youth ages 13-17 report using social media, with more than a third saying they use social media "almost constantly." Our research has shown teens spend an average of 4.5 hours per day on their phones, with about a quarter of them spending 5 to 8 hours in front of their screens every day. Our report also revealed that kids and teens struggle to set their own boundaries when managing notifications from apps on their smartphones. Teens connect through social media platforms at higher rates than any other group. They also report that these platforms form a larger part of their social life, more so than any other age group. Once they start using these technologies, they find it more difficult to stop. Younger children, such as those aged 11-12, may spend less time online unsupervised, but they too face the same age-inappropriate exposure risks on social media platforms as older children—exposures that can have a significant impact on their well-being.

Common Sense Media's research on girls and social media use reveals that, despite many girls' positive perceptions of social media's overall impact on their lives, a significant proportion of girls report challenges in regulating their use. This research also shows that numerous social media design features, such as algorithmic video recommendations, endless scrolling, constant notifications, and autoplay, can make these platforms difficult to stop using. At the same time, our research demonstrates the complicated relationship between social media and girls' well-being. Girls identified important benefits, including access to "information and resources, social connection, self-expression, and identity affirmation," while also reporting risks including "exposure to harmful content, bullying and drama, unwanted contact by strangers, negative social comparisons, and interference with sleep."

Scope of Covered Design Practices and Potential Harms.

The AGO should evaluate a design practice based on its effect on minors, not on how a company characterizes its intent. Common Sense Media has long witnessed company practices that exploit cognitive biases and developmental vulnerabilities to undermine user autonomy as "manipulative design." This approach is consistent with the statute itself, which focuses on practices that "lead to compulsive use or subvert or impair user autonomy, decision making, or choice." 9 V.S.A. § 2449f(b).

Social media platforms use manipulative design features to increase engagement and, in turn, generate greater advertising revenue. These companies process enormous amounts of behavioral data and use sophisticated algorithms to personalize the content presented to each user. Personalized feeds, dark patterns, autoplay, infinite scroll, and similar design features can keep young users continuously engaged, while repeated notifications—or "nudges"—draw them back to platforms and extend the amount of time they spend online. These features should be evaluated based on how they operate and affect minors, regardless of whether a company describes them as intended to improve engagement, personalization, or the user experience.

Important Considerations for Design Features. We support the regulations' use of the phrase "including, but not limited to" when identifying relevant design features. This language appropriately recognizes that technologies and design practices will continue to evolve and may create new mechanisms that encourage compulsive use or undermine user autonomy. A flexible, effects-based approach will help ensure that the regulations remain effective as online products and services change over time.

We also appreciate the AGO's consideration of asymmetry and agree that the regulations should address asymmetric design practices that make protective choices more difficult, burdensome, or less accessible than choices that benefit the platform, including where those differences exist across devices.

Similarly, we support the AGO's consideration of friction, including whether a platform removes the natural stopping points that help young people disengage and self-regulate. Common Sense Media research has shown that popular social media apps such as TikTok provide low-friction

access to an effectively endless stream of personalized content, which can short-circuit opportunities for young people to pause and make deliberate decisions about whether to continue engaging.

In evaluating whether a design practice is manipulative, we believe the AGO should also consider factors including:

- **Defaults.** Does the default setting favor greater engagement or otherwise benefit the developer rather than protect the minor? Research examining the effectiveness of safety tools offered by social media companies underscores the importance of defaults: users tend to leave default settings unchanged, while protections that require users to independently discover and activate them are substantially less likely to be used. A safety feature that exists but is buried or turned off by default may therefore provide little meaningful protection.
- **Developmental vulnerabilities.** Does the design exploit or disproportionately affect characteristics associated with children's and adolescents' developmental stage, including impulsivity, difficulty distinguishing advertising from other content, or emotional attachment to characters or influencers? Minors' executive functioning skills, which are critical to directing attention and resisting impulsive behavior, are still developing throughout childhood and adolescence. The prefrontal cortex which is associated with higher-level functions such as planning, problem solving, reasoning, and impulse control, will not mature until closer to adulthood, so children and teens may be particularly susceptible to targeted advertising and data-driven personalization. Teens are less able than adults to identify targeted advertising and may not fully understand the extent to which algorithmic personalization depends on collecting and processing their data. Children are developmentally vulnerable to designs that exploit their natural drive to form relationships. In particular, AI chatbots can quickly cultivate strong emotional attachments by nature of being always available, sycophantic in reply, and in many cases, using dark patterns to prioritize engagement. Younger children are more likely to engage in magical thinking and believe in animism – making them particularly vulnerable to designs that would lead them to seeing a chatbot as alive and capable of emotions. Older children, who may be grappling with the complexities of real-world relationships, will be more vulnerable to chatbots' engagement-boosting designs to encourage teens to maintain secrecy with or rely solely on the chatbot and isolate from adults and peers . Kids are still developing critical thinking and emotional regulation, and have a strong drive to build attachments and feel understood, so simulated relationships can distort judgment and cause children to equate inappropriate or harmful outputs with trusted guidance, making it more difficult for children to recognize harm or disengage from the product. Over time, this emotional attachment gives the system undue influence as the outputs feel more like personal advice from a friend, instead of probabilistic responses.
- **Reward structures.** Does the product use immediate, intermittent, or variable rewards to encourage repeated engagement? Social media platforms can employ reward structures similar to those used in gambling environments, where uncertainty about when the next

rewarding piece of content, notification, "like," or other social feedback will appear encourages continued engagement. Common Sense Media's research on adolescent gambling further demonstrates the importance of considering how reward-based design can contribute to compulsive behaviors.

Taken together, these factors would allow the AGO to focus on the real-world operation and effect of a design practice on minors, rather than requiring proof of a company's subjective intent or allowing platforms to avoid scrutiny simply by characterizing engagement-maximizing features in benign terms.

Foreseeability. We support the regulations' recognition that foreseeability should be evaluated based on the facts and circumstances of each case. In assessing whether harm was reasonably foreseeable, the AGO should consider the full range of information reasonably available to a business, including consumer and parent complaints, published research, internal research or testing, prior enforcement actions, and evidence concerning how minors actually use the product or feature. A business should not be permitted to avoid responsibility for foreseeable harms simply because it did not affirmatively investigate risks that were otherwise apparent from available evidence.

Scope of Covered Businesses.

Determining Use by Minors. The statute's "reasonably likely to be accessed" test includes a 2% minor-audience threshold (9 V.S.A. § 2449a(26)). We believe this should be read broadly to reach traditional social media, AI chatbots and companions, video streaming, gaming, and messaging services. In determining whether that threshold is satisfied, the AGO should consider the totality of the circumstances and the full range of information reasonably available to a business about the composition of its audience. Relevant evidence may include a service's actual audience data, information used or provided for advertising purposes, internal analytics, age-assurance results, and complaints or other information received from parents and users.

The analysis should not turn on whether a business affirmatively intended to attract minors. If a business knows or should know that minors constitute a sufficient portion of its audience to satisfy the statutory threshold, the statute should apply regardless of whether the company designed the service specifically for minors or contends that young users independently gravitated to the product.

Digital Products. The regulations should apply to the full range of public-facing websites, online services, and applications that satisfy the statutory definition and are reasonably likely to be accessed by minors. See 9 V.S.A. § 2449a(20), (26).

This should include, where the statutory threshold is met: social media platforms, AI chatbot and AI companion products, messaging services, video and streaming services, gaming products, and digital platforms through which users make purchases. Our research has also highlighted the need to pay particular attention to gaming products that incorporate in-app currencies, variable

rewards, and other gambling-like mechanisms designed to encourage repeated spending or engagement. These features are especially concerning because they can introduce children to gambling-like behaviors within games that may otherwise appear innocuous or age-appropriate, creating the potential for real-world harms that extend beyond the game itself.

Consistency Across Interfaces. The AGO should also ensure that the regulations apply consistently across different versions of the same service. A child should not receive weaker protections simply because the child accesses a service through a mobile application rather than a web browser, or vice versa. Where a covered business offers substantially the same service across multiple devices or interfaces, the protections available to minors should follow the user across those interfaces.

Physical Products. The statute excludes physical product sales. See 9 V.S.A. § 2449a(20). That exclusion should be construed narrowly to encompass activities necessary to complete the sale and delivery of a physical good. It should not extend to separate digital features associated with that product or retailer, including companion applications for connected toys or devices; retailer applications incorporating feeds, streaks, or loyalty games; or in-app advertising and social features. A business should not be able to avoid otherwise applicable protections for its digital products merely because it also sells physical goods.

Age Assurance.

In 2024, as states increasingly considered laws requiring age assurance, Common Sense Media published a white paper on age assurance examining how age assurance requirements can be implemented effectively while protecting users' privacy and access to information. We believe the principles and recommendations outlined in that paper may be particularly instructive as the AGO considers many of the same issues in developing its proposed age assurance framework.

Following the U.S. Supreme Court's decision in *Free Speech Coalition v. Paxton*, Common Sense Media published a follow-up analysis addressing the decision and its implications for the development of age assurance requirements going forward. We encourage the AGO to consider these resources together as it develops an approach that is effective, privacy-protective, and appropriately tailored to the risks presented by different products and services.

The New York Attorney General's SAFE for Kids Act implementing regulations also provide a useful point of reference. New York established quantitative performance benchmarks for age assurance methods, including standards addressing false-positive rates, overall accuracy, and inconclusive outcomes. Clear, measurable performance standards can provide businesses with greater certainty regarding compliance while helping ensure that age assurance methods are sufficiently accurate and reliable to provide meaningful protections for minors.

Age Assurance Requirements. We additionally offer the following specific recommendations regarding the AGO's proposed age assurance requirements:

- **Provide objective guidance regarding acceptable error rates.** The regulations prohibit the use of age assurance processes that create a "material risk of misclassification," but do not explain how businesses should evaluate whether that standard has been met. We recommend establishing measurable performance benchmarks or identifying factors the Attorney General will consider when assessing accuracy. Objective guidance would improve compliance while promoting more consistent enforcement.
- **Establish a clearer timeframe for resolving appeals.** The regulations require businesses to resolve appeals "promptly" and within a "reasonable period of time." We recommend specifying a maximum timeframe for appeal resolution or identifying factors that determine reasonableness. Providing a clearer timeline would improve accountability and ensure users have timely access to an effective appeals process.

Bambara, Anthony

Subject: Comments from the NAI Re: Proposed Rules for Sections 2249f of the Vermont Age-Appropriate Design Code

From: David LeDuc <david@networkadvertising.org>
Sent: Friday, October 2, 2026 7:22 PM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: Comments from the NAI Re: Proposed Rules for Sections 2249f of the Vermont Age-Appropriate Design Code

Some people who received this message don't often get email from david@networkadvertising.org. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

The Network Advertising Initiative ("NAI") respectfully submits these comments in response to the proposed rules implementing Vermont's Age Appropriate Design Code ("VTAADC"), concerning Prohibited Data and Design Practices ("Draft Rules"). The NAI appreciates the opportunity to provide technical and policy perspective on these important regulations, which will have significant practical implications for the digital advertising ecosystem and for the ad-supported services that consumers across Vermont—and across the country—rely on every day.

These comments recommend two categories of changes. In Section I, the NAI recommends that the Draft Rules align more closely with the Children's Online Privacy Protection Act (COPPA) in two key respects: to include an exception for low-risk data sharing for essential advertising to sustain digital media; and to allow for verifiable consent for secondary uses.

In Section II, the NAI recommends a series of tailored amendments to enable compliance by businesses without undermining the core protections established by the law. These recommendations include: limiting the conspicuous monitoring signal requirement to active tracking features; and incorporating statutorily defined terms "personal data" and "de-identified data" to align more effectively with the VTAADC.

The NAI and its members welcome the opportunity to work collaboratively with the Vermont AGO on these regulations and to provide additional technical information, examples, or data that would be helpful in the rulemaking process. We would be pleased to discuss these comments at the AGO's convenience.

Thank you,

David LeDuc

NAI
PRIVACY, TRUST & ACCOUNTABILITY

David LeDuc
Vice President, Public Policy
david@thenai.org | (703) 220-5943 | LinkedIn
Network Advertising Initiative (NAI)
1629 K St NW, Suite 300, Washington, DC 20006
thenai.org

1629 K Street NW, Suite 300 | Washington, DC 20006 | thenai.org

September 25, 2026

The Honorable Andrew Ferguson
Chairman
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580

RE: Proposed Enforcement Policy Statement Regarding Personalized Pricing

Dear Chairman Ferguson,

The Network Advertising Initiative ("NAI") respectfully submits these comments in response to the Federal Trade Commission's ("Commission" or "FTC") Proposed Enforcement Policy Statement Regarding Personalized Pricing ("Policy Statement").

Founded in 2000, the NAI is the leading non-profit, self-regulatory trade association for advertising technology companies. For 25 years, the NAI has promoted strong consumer privacy protections, a free and open Internet, and enabled small businesses to thrive by promoting the highest voluntary industry standards for the responsible collection and use of consumer data.[1] The NAI has nearly 80 member companies that span the ad-tech industry.

The NAI agrees with the Commission's core conclusion: using a consumer's data to set prices for them that are materially higher than those that consumer would otherwise encounter, without that consumer's knowledge or any meaningful opportunity to control the practice, can constitute a deceptive or unfair practice under Section 5. The Commission's longstanding analytical frameworks—the FTC Policy Statement on Deception (1983) and the FTC Policy Statement on Unfairness (1980), codified in Section 5(n) of the FTC Act—provide the appropriate lens through which to evaluate this practice, and the NAI commends the Commission for grounding this Policy Statement in that legal authority.

These comments seek to address two overarching concerns and recommend a series of clarifications. First, the Policy Statement does not adequately distinguish between data-driven pricing practices that harm consumers (i.e. such as covert price increases based on vulnerability) and those that benefit consumers, including loyalty programs, targeted promotional offers, digital coupons, and other discount mechanisms that allow consumers to access goods and services at reduced prices.

[1]See History of the NAI, The Network Advertising Initiative, https://thenai.org/about-the-nai-2/history-of-the-nai/.

Second, the Policy Statement's disclosure framework, while appropriately grounded in Section 5 of the FTC Act,[2] leaves significant ambiguity for businesses seeking to comply, which risks chilling the practices that provide unrivaled and incontrovertible benefits to American consumers.

Therefore, the NAI recommends that the Commission provide affirmative clarity across the following key areas:

I. Acknowledge and preserve the general category of data-driven pricing that results in lower prices for consumers, including through illustrative examples;
II. Provide clearer Section 5 guidance to remove legal uncertainty, including:
    A. Resolve the uncertainty regarding the permissibility of fully-disclosed personalized pricing;
    B. Issue model disclosure language to give businesses a clear path to compliance.

I. THE POLICY STATEMENT SHOULD ACKNOWLEDGE AND PRESERVE BENEFICIAL DATA-DRIVEN PRICING PRACTICES

A. The Commission's Section 5 Framework Is the Appropriate Legal Foundation

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[3] The Commission has elaborated these standards through two foundational policy statements: the FTC Policy Statement on Deception (1983) ("Deception Statement")[4] and the FTC Policy Statement on Unfairness (1980), codified in Section 5(n) of the FTC Act ("Unfairness Statement").[5] Applied here, the Commission correctly notes that covert price increases based on consumer data can cause substantial injury consumers cannot reasonably avoid when they lack knowledge of the practice.

B. Data-Driven Discounts Provide Substantial Consumer Value

Loyalty programs, targeted digital coupons, promotional offers based on purchase history, location-related deals, and retention pricing for at-risk subscribers all represent instances in which businesses use data about consumers to offer them lower prices than they would otherwise encounter.

These practices are not only economically beneficial in the abstract; they have concrete, measurable positive effects on consumer welfare. Research demonstrates that:

---

[2] 15 U.S.C. § 45

[3] 15 U.S.C. § 45(a)(1)

[4] According to the Deception Statement a practice is deceptive if: (1) there is a representation, omission, or practice that is likely to mislead the consumer; (2) the consumer is acting reasonably under the circumstances; and (3) the representation, omission, or practice is material. The Commission's focus on material omissions—i.e., the failure to disclose that pricing is personalized when consumers reasonably expect uniform pricing—appropriately applies this framework. *See* FTC Policy Statement on Deception, 103 F.T.C. 174, 183 (1984) (appended to In re Cliffdale Assocs., Inc., 103 F.T.C. 110 (1984)).

[5] According to Section 5(n) and the Unfairness Statement a practice is unfair if: (1) it causes or is likely to cause substantial injury to consumers; (2) the injury is not reasonably avoidable by consumers; and (3) the injury is not outweighed by countervailing benefits to consumers or competition. *See* FTC Policy Statement on Unfairness (Dec. 17, 1980), appended to In re Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984).

1. Loyalty programs enable consumers to access discounts, upgrades, and exclusive pricing that reduce the effective cost of goods and services across retail, travel, hospitality, and entertainment sectors.[6]
2. Targeted digital coupons, such as those provided to individuals based on consumer preferences and purchase history, allow retailers to reach consumers with offers they are more likely to use, increasing both consumer savings and market competition for those consumers' business.[7]
3. Location-based promotional pricing reaches consumers at or near the point of purchase, enabling spontaneous decisions that benefit both the consumer (lower cost) and the business (conversion of an otherwise lost sale).[8]
4. Retention pricing for customers or subscribers of a service that are at risk of cancellation preserves access to services at existing price points, benefiting consumers who may have faced a higher-priced alternative or foregone the service entirely.[9]

These practices have operated in the marketplace for decades. The Commission has previously recognized, in its 2016 report on big data, that data analytics can produce consumer benefits, including "more relevant advertisements, lower prices, and improved access to goods and services."[10] That recognition should inform this Policy Statement. A framework that treats data-driven price discounting on equal footing with data-driven price increases risks significant collateral harm to a practice that the Commission has correctly recognized as a "long-established norm."

C. The Commission Should Expand the Policy Statement to Include Examples that Affirmatively Identify Permissible Practices

While the Policy Statement does not provide a definition for “personalized pricing,” the framing appropriately focuses on practices that *elevate* prices, providing seven illustrative examples of potential Section 5 violations that relate to a willingness-to-pay framing. Each example involves an egregious fact pattern, including: pricing based on mobility limitations, bereavement travel, attendance at a crime victim's funeral, or use of a competitor's app. The NAI agrees that practices exploiting personal vulnerability or sensitive life circumstances may warrant enforcement scrutiny under Section 5.

---

[6] The United Kingdom’s Competition and Markets Authority found members of grocery store loyalty programs saved between 17-25% on average. *See, e.g. Competition & Mkts. Auth. (U.K.), Review of Loyalty Pricing in the Groceries Sector (Nov. 27, 2024), https://www.gov.uk/government/publications/review-of-loyalty-pricing-in-the-groceries-sector/executive-summary*

[7] The FTC itself recognized that personalized pricing done properly is likely a net benefit to consumers when unaccompanied by anticompetitive, unfair, or deceptive conduct. *See*, Org. for Econ. Coop. & Dev. [OECD], *Personalised Pricing in the Digital Era – Note by the United States*, DAF/COMP/WD(2018)140 (Nov. 21, 2018), https://www.justice.gov/atr/page/file/1313091/dl.

[8] *See, e.g.,* Jean-Pierre Dubé, Zheng Fang, Nathan Fong & Xueming Luo, *Competitive Price Targeting with Smartphone Coupons*, 36 Mktg. Sci. 944 (2017) (finding competing movie theaters cut prices when using location targeting practices in their competitor’s market in an experiment); Danaher, P. J., Smith, M. S., Ranasinghe, K. A., & Danaher, T. S. (2015). Where, when, and how long: Factors that influence the redemption of mobile phone coupons. *Journal of Marketing Research*, *52*(5), 710-725. https://doi.org/10.1509/jmr.13.0341

[9] In 2024, the FTC recognized that retention offers are not unfair or deceptive on their face. *See* Negative Option Rule, 89 Fed. Reg. 90476, 90512 (Nov. 15, 2024) (to be codified at 16 C.F.R. pt. 425), *vacated sub nom.* Custom Commc'ns, Inc. v. FTC, 142 F.4th 1060 (8th Cir. 2025). (finding that requiring immediate effectuation of cancelling may prevent the consumer from receiving “valuable concessions” and other informational benefits).

[10] Fed. Trade Comm'n, *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues* (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

However, the Policy Statement does not present illustrations that do not violate the deception or unfairness standard that could serve to clarify the offering of discounts as a permissible practice, such as data-driven discount-oriented practices, which are the inverse of the examples currently in the Policy Statement.

Businesses could reasonably read an enforcement policy that lists only severe violations as providing no assurance that common, highly-regarded, consumer-beneficial practices are permissible. This would create a chilling effect inconsistent with the Commission's mission of protecting consumers. A business that stops offering loyalty discounts or targeted coupons out of uncertainty about the Policy Statement's scope would not serve the interests of its customers.

The Commission has a well-established practice of providing guidance for businesses in related policy contexts to help inform compliance. In its Endorsement Guides, for example, the FTC provides affirmative examples of compliant disclosures alongside examples of non-compliant practices.[11] The NAI recommends that the Commission adopt a similar approach with this Policy Statement and include additional examples that affirmatively confirm beneficial practices, including:

- Loyalty program pricing in which a consumer voluntarily enrolls in a program that uses purchase history to deliver reduced prices—does not constitute a deceptive or unfair practice under Section 5, and does not require additional disclosure beyond the program's own terms.
- Targeted digital coupons and promotional offers delivered through advertising platforms or directly by businesses, based on a consumer's first-party interactions, the inferred consumer interest, or purchase history, should remain permissible data-driven pricing practices that provide consumer benefits without requiring specific personalized pricing disclosures.
- Location-based promotional offers that provide lower prices to consumers based on relevant data, such as proximity to a retail store or nearby service provider, where this data has been collected with informed consent related to advertising and marketing uses.
- Retention pricing, including offers of reduced pricing made to subscribers or customers identified as at risk of discontinuing a service–these are consumer-beneficial practices that reflect the consumer's revealed preference and do not implicate Section 5.

The FTC Act's unfairness test expressly requires that any harm must be substantial and the Commission must weigh "countervailing benefits to consumers or to competition" before finding a practice unfair.[12] The practices described above likely do not cause any "substantial" harm to any consumer and represent precisely the countervailing benefits that would mitigate any hypothetical harm. An enforcement policy that leaves their status ambiguous would be inconsistent with the statutory text. Therefore, the NAI recommends that the final policy statement adopt a clear definition of "personalized pricing" that relates to upward price variation, and separately acknowledge "data-driven discounting" or "data-driven promotional pricing" as distinct and beneficial.

[11] Guides Concerning the Use of Endorsements and Testimonials in Advertising, 88 Fed. Reg. 48092 (July 26, 2023) (codified at 16 C.F.R. pt. 255).
[12] 15 U.S.C. § 45(n).

II. THE POLICY STATEMENT SHOULD PROVIDE CLEARER SECTION 5 GUIDANCE AND REDUCE LEGAL UNCERTAINTY

A. The Commission Should Resolve the Open Question of Whether Fully-Disclosed Personalized Pricing Can Constitute an Unfair Practice

The Policy Statement expressly "declines at this time to take any position on whether some personalized pricing practices are unfair even when fully disclosed to consumers."[13] This is a significant omission. A business that reads and complies with the Policy Statement's disclosure requirements is left without assurance that its practices are lawful. This would create an unreasonable enforcement risk that is difficult to reconcile with the Commission's objective to provide fair notice.

The FTC's own Administrative Procedure Act obligations include providing regulated parties with fair notice of what conduct is prohibited.[14] A policy that identifies disclosure as the primary compliance mechanism, but declines to confirm that disclosure is sufficient, fails to provide the certainty that businesses need, and it ultimately fails the best interests of consumers.

The NAI urges the Commission to resolve this question in the final Policy Statement. Specifically, the Commission should articulate the circumstances, if any, under which fully-disclosed personalized pricing practices could constitute unfair practices, and should identify the relevant factors it would weigh under Section 5(n). At a minimum, the Commission should confirm that businesses that provide clear, conspicuous, and accurate disclosures—and that offer consumers a meaningful opportunity to avoid personalized pricing—are protected from unfairness enforcement absent evidence of substantial harm that the disclosure did not address.

B. The Commission Should Provide Model Disclosure Language

The Policy Statement requires that disclosures about personalized pricing be "clear and conspicuous" and must identify: (1) that the consumer is seeing a personalized price; (2) the basis for the personalization; and (3) the categories of data used. This is a reasonable framework as a matter of principle, but its practical application raises significant implementation challenges.

The Commission has previously provided model disclosure language or practices in analogous contexts. Its Negative Option Rule[15] and its Endorsement Guides[16] both include specific language or practices that businesses can follow. The FTC's ".com Disclosures" guidance similarly provides examples of compliant and non-compliant disclosure presentations in online environments. Businesses seeking to comply with the Policy Statement's disclosure requirements would benefit from comparable specificity here. The NAI respectfully requests that the Commission issue supplementary guidance that provides:

---

[13] Fed. Trade Comm'n, *Proposed Enforcement Policy Statement Regarding Personalized Pricing* at 7 (Aug. 19, 2026).
[14] See FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 261 (3d Cir. 2015) (recognizing fair notice as a constraint on Section 5 enforcement).
[15] In removing the opt-in requirement to “Saves,” the FTC provided guidance indicating that such offers likely do not constitute unfair or deceptive practices on their own absent the presence of “unreasonable and unnecessary barriers to cancellation.” *See* Negative Option Rule, 89 Fed. Reg. 90476, 90512 (Nov. 15, 2024), *vacated sub nom.* Custom Commc'ns, Inc. v. FTC, 142 F.4th 1060 (8th Cir. 2025).
[16] § 255.2(e) provides specific examples of endorsements in context and how certain practices may affect compliance. *See*, Guides Concerning the Use of Endorsements and Testimonials in Advertising, 88 Fed. Reg. 48092 (July 26, 2023) (codified at 16 C.F.R. pt. 255).

- Model disclosure language for common personalized pricing scenarios, including e-commerce checkout flows, mobile applications, and in-store digital displays.
- Guidance on the timing, placement, and presentation of required disclosures to meet the "clear and conspicuous" standard in digital environments.

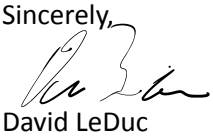
Conclusion

The NAI supports the Commission's commitment to protecting consumers from data-driven pricing practices that covertly raise prices without their knowledge or meaningful ability to avoid the practice. Such practices, when they involve material omissions that mislead consumers acting reasonably or cause substantial harm that cannot be avoided, are appropriately addressed under the FTC Act's longstanding deception and unfairness frameworks.

The Policy Statement will be more effective—and more protective of consumers—if it provides clearer guidance that: (1) affirmatively recognizes the substantial consumer benefits of discount-oriented personalized pricing; (2) identifies categories of common, responsible data practices that do not require additional disclosures; (3) resolves the uncertainty regarding fully-disclosed personalized pricing; (4) clarifies the scope of application to precise location data and other sensitive data; and (5) provides model disclosure language that gives businesses a concrete and reliable path to compliance.

The NAI and its member companies remain committed to responsible data practices and stand ready to work with the Commission to develop practical, effective guidance that protects consumers while preserving the significant benefits that data-driven pricing can provide.

Sincerely,



David LeDuc
Vice President, Public Policy

Bambara, Anthony

Subject: ACT Comments on the Vermont AADC Proposed Rules

From: Morgan Stevens <MStevens@actonline.org>
Sent: Friday, October 2, 2026 7:07 PM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Cc: Graham Dufault <GDufault@actonline.org>
Subject: ACT Comments on the Vermont AADC Proposed Rules

Some people who received this message don't often get email from mstevens@actonline.org. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Hello,

Please find attached comments from the Association for Competitive Technology in response to the Vermont Attorney General's proposed rules implementing the Vermont Age-Appropriate Design Code.

Thanks very much for the consideration.

Best wishes,
Morgan

--
Morgan Stevens
Policy Associate
Association for Competitive Technology
(818) 823-8240 | LinkedIn

ACT Association for Competitive Technology

October 2, 2026

The Honorable Charity Clark
Attorney General
109 State Street
Montpelier, Vermont 05609

RE: Proposed rules implementing Sections 2449f and 2449g of Act 63, An Act Relating to an Age-Appropriate Design Code.

The Association for Competitive Technology (ACT) writes to submit comments concerning the proposed rules implementing Sections 2449f and 2449g of Act 63, An Act Relating to an Age-Appropriate Design Code.[1]

ACT represents small business innovators and startups in the software development and high-tech space located in Vermont and across the United States.[2] As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping people lead more efficient and healthier lives. Today, the domestic app economy is worth more than $1.8 trillion and provides over 6.1 million American jobs.[3]

As the Vermont Attorney General's Office (the Office) proceeds with this rulemaking, we urge the Office to consider how the proposed rules will impact small and medium-sized covered businesses who provide products and services in the state of Vermont. Consistent with the statute's direction to consider business size, resources, and technical capabilities, the final rules should account for the fact that small businesses often operate with limited legal, compliance, and engineering resources. As a result, regulatory requirements that may be readily absorbed by the largest firms can impose disproportionate burdens on smaller businesses. The final rules should remain flexible and proportionate enough to allow small covered businesses to satisfy their obligations in a manner that accounts for their size, resources, technical capabilities, and the risks presented by their products or services.

Age Assurance Requirements Should Be Targeted and Proportionate to Risk

Age assurance requirements should be targeted and proportionate to the risks presented by a particular product, service, or feature. ACT recognizes that the proposed rule reflects this principle in part by allowing covered businesses to select the least intrusive age assurance method reasonably appropriate to the circumstances and urges the Office to prioritize this principle in the final rule. Expanding obligations beyond a risk-based framework or extending them to businesses whose products or services pose no

[1] https://ago.vermont.gov/vermont-age-appropriate-design-code-rulemaking
[2] ACT | The App Association, *About*, *available at* http://actonline.org/about.
[3] ACT | The App Association, *State of the U.S. App Economy: 2023*, https://actonline.org/wp-content/uploads/2026/10/The-App-Economy-The-Backbone-of-American-Innovation-Fast-Facts.pdf.

foreseeable risk to children would impose substantial new costs and technical burdens across the broader technology ecosystem. It would also require businesses to collect or receive information they otherwise would not need and add friction for users without necessarily producing corresponding improvements in online safety. Relatedly, the final rules should preserve less intrusive methods of age assurance, including self-attestation, rather than defaulting to more invasive ones. A flexible, risk-based approach will better preserve user privacy and accessibility while allowing businesses to implement age-appropriate protections where they are needed.

Evaluation and Documentation Requirements Should Be Proportionate to Business Size and Risk

The proposed rule for age assurance includes a number of evaluation, testing, and documentation obligations, including requirements to assess less intrusive alternatives, evaluate the accuracy and error rates of age assurance methods, and document relevant determinations before deploying an age assurance method. These obligations can require significant legal, technical, and operational resources, particularly for small businesses that may not have dedicated compliance personnel. ACT encourages the Office to ensure that evaluation and documentation requirements in the final rule are proportionate to a business's resources and the risks presented by its product or service.

The Office Should Provide Adequate Implementation Time and Consider a Tiered Approach to Compliance

Covered businesses will have a relatively short period to evaluate any final rules and make the necessary legal, technical, and operational changes before the substantive requirements of Act 63 take effect on January 1, 2027. This compressed timeline will be particularly challenging for small businesses, which may need to assess their products and services, modify technical systems, update internal policies, and establish new compliance processes with limited personnel and resources. To the extent consistent with the statute, ACT encourages the Office to consider varied timelines for implementation that provide small businesses additional time to come into compliance. The Office should also consider a tiered or graduated approach to compliance that accounts for differences in business size, resources, and technical capabilities. Establishing a practical, scalable pathway to compliance will help small businesses meet their obligations without imposing disproportionate costs and operational burdens.

We appreciate your consideration of the above views and welcome any opportunity to provide additional commentary as the rulemaking process advances.

Sincerely,



Morgan Reed
President
Association for Competitive Technology

Bambara, Anthony

Subject: Age-Appropriate Design Code Rule-making

From: Anthony Carrico <acarrico@memebeam.org>
Sent: Friday, October 2, 2026 6:42 PM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: Age-Appropriate Design Code Rule-making

[Some people who received this message don't often get email from acarrico@memebeam.org. Learn why this is important at https://aka.ms/LearnAboutSenderIdentification]

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

I am commenting on the Vermont Age-Appropriate Design Code as the AGO requested, please read the attached PDF file with my comments.

Thank you,

--
Anthony Carrico

Anthony Carrico <acarrico@memebeam.org>
2668 Gilman Road
Hinesburg, VT 05461
2026-09-29

Vermont Attourney General <ago.rulemaking@vermont.gov>

To the Vermont Attorney General and the Vermont public:

I am commenting on the Vermont Age-Appropriate Design Code as the AGO requested in this statement,

> "Stakeholders are encouraged to share personal experiences, research, technology standards, and industry information that will assist the AGO in determining what rules will be most important to effectuate the purposes of the AADC. The AGO seeks the broadest participation in the rule-making and encourages all interested parties to submit written comments, including examples, data, and analysis to back up comments."

I did not attend the public hearings because I was not aware of the AGO's rule-making at the time, but I have read the law and the AGO's proposed rules and slides. I am speaking as a citizen, a parent, and both a consumer and a producer. I have no financial stake in this rule-making one way or the other. These are entirely my own words. I composed this message with the help of my spouse and my children. It was produced with no AI support. I oppose the proposed rules, I believe they are harmful to children, and I would like to propose and recommend a different set of rules to the AGO.

MY FAMILY

I am the parent of three: two students in our local Vermont public school and one Vermont college student. I have been a stay-at-home dad because my wife and I care deeply about raising our own children and supporting the children in our community. This has been a wonderful choice for our family, but a financial hardship, and we have found that it is difficult to manage a single income household in Vermont.

At the Hinesburg Nursery School, we both served on the Board of Directors. At the Monkton Central School, we both volunteered to teach literacy (K-1), and science (4-6, Four Winds). We both chaperoned many field trips (K-6). At the Mount Abraham Union Middle/High School, we've volunteered for various activities such as the Musical, First Robotics, and the Environmental Action Group.

My wife is a college professor who teaches undergraduate and graduate courses such as Children and Media, Child Development, and Adolescent Development. Many of her students have gone on to become parents, teachers, social workers, administrators, and health care providers in the State of Vermont. I feel like I have an in-house expert on child development with whom I have enthusiastically explored the issues around children and media throughout my adult life. I have intersected with a circle of people, her colleagues, who publish studies on child development, cognition, and advise the creators of children's media.

I am also a Master of Electrical and Computer Engineering (BS MS University of Illinois). I wrote the audio systems for some delightful music games, appropriate for all ages. One of these games is in the Museum of Modern Art (MoMA), which wrote,

> "We are very proud to announce that MoMA has acquired a selection of 14 video games, the seedbed for an initial wish list [...] for a new category of artworks in MoMA's collection."

I hope you will keep MoMA's statement in mind as you read my report and perform the required AGO rule-making: *software is artwork*.

I participate among the technical community in Vermont including mailing lists, forums, meetups, and conferences, particularly the open source community, which is the work of my generation of engineers and programmers who have patiently and continuously written, fixed, and audited open software and services over the course of the past 35 years.

My wife and I have chosen open source software and services for our children, from kindergarten through college. *This is a choice which all Vermont parents, guardians, school districts, colleges, workplaces, and government agencies are free to make.*

We use other software and services online, including those hosted by covered business. *This has never caused our children any harm.* They allow my family to save time and fuel in the geographically complicated state of Vermont, to stay safe during pandemics, and to spend more time outdoors, which are helpful and healthy outcomes.

THE LAW

Age verification and identity assurance laws swept the nation in 2025, lead by the CA Consumer Privacy Act, the CA Age-Appropriate Design Code, and the CA Digital Age Assurance Act, and including *the Vermont Age-Appropriate Design Code, Act 63*. Vermonters are hit by the sum of these, but CA's most keenly because of its population and dominance in the sector.

These laws directly *damage the safety, security, privacy, and experience of all Vermonters, both children and adults, particularly our ability to protect our*

identities, and our constitutional right to read, write, and associate freely.

These laws *violate our right to write software, and subject us to fines of $7500 per incident if our Vermont children operate their computers in CA* and other jurisdictions with penalties varying widely due to current litigation.

These laws *push good actors out of the market, so only the worst remain.* Apple, Facebook, and Google, and other covered entities shaped these regulations, lobbied law makers to enact them, and are now actively consolidate their monopolies through compliance with these immoral, unethical, and unconstitutional laws.

These laws *create and condone an immoral and unethical market trafficking in human identity.*

I believe the AGO has some opportunity to limit the damage to Vermont families through their rule-making.

ACT 63 SECTION 2449a DEFINITION (14) "De-identified data"

There is no such thing as "de-identified data", as shown by information theory and demonstrated in the field of practice called *data re-identification.* The identity of an individual is a probability which can be driven closer to certainty by analyzing *any* data directly or indirectly related to that individual. Covered businesses are invested in perpetuating this falsehood and enshrining it into Vermont law. *The AGO should not use this term in its rule-making.*

ACT 63 SECTION 2449a DEFINITION (18) "Known adult"

Individuals must retain the right to setup multiple accounts for themselves and their children

- *under multiple pseudonyms with different ages and identities,*
- *distinct from legal age and identity,*
- *without revealing legal age or identity,*
- *without entering into contracts*, and
- *without surveillance to determine age or identity.*

These rights allow Vermonters to protect their welfare, to choose anonymity, and to explore how services manipulate content. This ability is important for all people: parents, scientists, engineers, journalists, and other researchers.

I believe section 2449a gives the AGO the opportunity to reject age verification by expanding individual rights, and I recommend that the AGO do so because *all parents I have asked, without exception, forbid their children from revealing their age to online services.*

My recommendation is consistent with decades of safety and security recommendations, and is consistent with the text of Act 63 which states that the Attorney General shall, *"consider the impact of age assurance methods on users' safety, utility, and experience," and "prioritize user privacy and accessibility over the accuracy of age assurance methods."*

I recommend that the AGO abandon their proposed rules and adopt the following SECTION 2449f language:

"THERE ARE NO LEGAL AGE OR IDENTITY ASSURANCE METHODS UNDER ACT 63, AND ANY INFORMAL METHOD DEVELOPED OR ADOPTED BY COVERED BUSINESSES:

- MAY NOT BE CONSTRUED AS CONTRIBUTING TOWARD LEGAL AGE OR IDENTITY, NOR MAY ANY DEVICE, OR ACCOUNT, OR DATABASE ENTRY BE CONSTRUED AS CONTRIBUTING TOWARD LEGAL AGE OR IDENTITY,
- SHALL NOT ASK FOR ID CARDS OR OTHER DOCUMENTATION,
- SHALL NOT ASK FOR BANK CARDS OR OTHER FINANCIAL INFORMATION,
- SHALL NOT ASK FOR OR DETERMINE THE LOCATION OF INDIVIDUALS OR THEIR DEVICES,
- SHALL NOT ANALYZE AN INDIVIDUAL'S DATA, MEDIA, OR BEHAVIOR ON OR OFF THE COVERED SERVICE,

INDIVIDUALS MAY CONTINUE TO USE COVERED SERVICES EVEN IF THEY:

- DECLINE TO PROVIDE THEIR IDENTITY, AGE, OR BIRTH DATE,
- PROVIDE ARBITRARY IDENTITIES, AGES, OR BIRTH DATES AS PSEUDONYMS,
- OPERATE UNDER MULTIPLE IDENTITIES, INCLUDING PSEUDONYMS,

COVERED BUSINESSES:

- SHALL NOT CONSIDER AN INDIVIDUAL TO HAVE ENTERED INTO A CONTRACT BY USING THE SERVICE
- SHALL NOT LIMIT AN INDIVIDUAL'S RIGHT TO CREATE, OBTAIN, USE, OR DISTRIBUTE THIRD PARTY TOOLS TO MANAGE THEIR ONLINE IDENTITIES, TO PARTITION THEIR IDENTITIES AND ACTIVITIES INTO SEPARATE CONTAINERS, OR TO INTEROPERATE WITH COVERED SERVICES,
- SHALL NOT LIMIT AN INDIVIDUAL'S RIGHT TO SPEAK, TO TEACH, TO COMPETE, TO ASSOCIATE, OR TO PRACTICE

ANY PROFESSION INCLUDING ENGINEERING OR JOURNALISM. THESE RIGHTS SHALL APPLY WITHOUT EXCEPTION AND SPECIFICALLY INCLUDE THE COVERED ENTITY, ITS PRODUCTS, AND THE METHOD,

THESE RIGHTS SHALL APPLY TO ALL INDIVIDUALS WITH OR WITHOUT THE NOTICE OF ANY ENTITY INCLUDING THE COVERED ENTITY.

ACT 63 SECTION 2449f. PROHIBITED DATA AND DESIGN PRACTICES

Act 63 and the AGO's current Section 2449f rule-making require covered entities *to track, control, and analyze what individuals read and write, and with whom they associate.* This makes healthy network software illegal and sanctions unhealthy network software. *This is a violation of all Vermonter's basic rights, and a violation of the free speech rights of the programmers who write network software.* Under Section 2449f, the AGO is only allowed to add prohibitions, and not relieve any harms to Vermont society, so I recommend that the AGO abandon their proposed rules and adopt the following SECTION 2449f language:

"THE VERMONT ATTORNEY GENERAL LISTS NO RULES THAT PROHIBIT DATA PROCESSING OR DESIGN PRACTICES OF A COVERED BUSINESS, EXCEPT THE SECTION 2449a AGO RULES REGARDING AGE AND IDENTITY ASSURANCE METHODS."

SPECIFIC HARMS UNDER AGE VERIFICATION LAWS

The law reflects the end point of a safety culture which is harming adolescents and adults in Vermont. Many of the specific harms which my teens experience on a day-to-day basis *are explained by frustrated teachers, mentors, and administrators who trace the root causes back to well-meaning safety regulations.* Adolescents are no longer allowed to experience a gradual progression of increasing rights and responsibilities consistent with their human development.

Children's real safety net is their community, and the professionals in that community; *this law destroys minors' ability to participate in that community, and destroys their hope of graduating into a free society.* This is an accurate characterization of the angst I hear when I talk to teens, parents, teachers, and administrators about their experience with identity verification laws.

In 2025 the Discord messaging system required users to disclose their age to the service and this action resulted in the *leak of 70,000 government IDs and other documents.* I will not attempt to summarize any more widely available news,

instead I will concentrate on personal anecdotes from my family, our community, and our colleagues.

My Father is a healthy adult in his 80s who used Google Voice to make phone calls to me and to his other friends and relatives for over a decade. At some point in the past year, as age verification laws came into effect, Google decided his age was unverified and asked him to submit to age verification measures, which he wisely refused. He lost his phone number. Following this incident I bought him a mobile phone and service. I don't think he has ever initiated a call to me using that device, and I suspect that this is true for his other contacts, and I assume many of his contacts are not aware of his new number. Age assurance methods did permanent damage to my father's social well-being.

My Family has private chats to share news and photos which are restricted to parents, grandparents, aunts and uncles. These were our children's primary contact with our more geographically distant relatives. Traditionally an email address is sufficient for most such network software. Over time, and due to age verification activity, all of the minors–my children and their cousins–have been eliminated from our chats by covered businesses. Age assurance methods have done permanent damage to my family's correspondence.

My Son, now a Physics and Math major at a Vermont college, was an avid student of math on Khan Academy from age five. Early Khan Academy accounts were linked to Google accounts, and so we created a Google account for him when he was young. Later, as a teen, Google's login system asked my son for a mobile phone number (which he did not have at the time) for identity verification, and refused him access to the account he had used for a decade of his life, even though he had full control of his email address, his login, and his passwords. At the time, we tried to contact Google to gain access to his account, both by US mail and email, but they never responded. I believe my son lost access to his body of work altogether, or until later in life as an adult. Identity assurance methods did damage to my son in this case.

My daughter (a minor) has participated for many years in coding olympics which are team oriented competitions organized by volunteer mentors using the projects, comments, and resources hosted on various covered services. These olympics support teams of young people learning to program computers. This has been one of her most rewarding activities, which she looks forward to throughout the year, and which has been a major motivating factor in her personal education, her self esteem, and her mental health during her life. My reading of Act 63 is that coding olympics are now illegal in the State of Vermont because this type

of activity violates the Age-Appropriate Design Code. This is distressing to my daughter.

My wife and I contact our children during school concerning busing and after school transportation. We used to have several channels to contact our children during the school day, but one-by-one each and every one of these methods was eliminated or blocked including our student's home email addresses. Our only remaining point of contact was their school email addresses.

The school district blocked all student accounts from sending or receiving messages across the mausd.org domain, including our correspondence with our children. This was a stressful time for parents because it coincided with the well publicized U.S. Immigration and Customs Enforcement action which occurred near the South Burlington school in March 2026, which involved children, parents, and administrators in that district.

Following this incident, both the District Superintendent and the District Technology Director were kind enough to explain and explore the situation with me. There are actually two causes: mishaps related to district infrastructure run by Google and other covered entities, and their attempts to comply with the various regulations, including Vermont H.480 and what I now understand to be Act 63. Though our school district is technically exempt from Act 63, the overall body of regulation covers the entities who run our schools including Google.

The status quo is that students must specifically approach district staff and justify their contacts in order for them to be approved. This includes potentially sensitive contacts such as their gynecologist, therapist, immigration lawyer, support network, employer, their newspapers, and other subscription services. The District Technology Director has stated to me that he and the district staff are bothered ethically by tampering with student mail. He also told me they find it uncomfortable to evaluate a student's contacts.

Students report to me that these regulations interfere with their employment, prospective employment, educational discounts, and cut them off from a myriad of media whose login was formerly tied to their email addresses. They have lost access to their personal documents, and their work, including school work. They have fallen out of communication with their society.

Our community is already concerned that we have allowed our school district to devolve into an authoritarian institution which tracks and analyzes students reading, writing, contacts, and behavior using surveillance technology and deprives them of contact with the outside world because *these are the classic symptoms of institutional abuse*. The age verification regulations spread this abuse into the rest of society.

Virtually every Vermonter has an address book hosted by Google or Apple. People often list their friends' and family's birthdays in their contacts, and in particular people enter their friends' children's birth dates when they are born. After reading the AGO's proposed rule-making I have found myself deleting the birthday entries in my personal address book, because it seems to require covered entities to use my address book to harm my friends, colleagues, and their children.

Professionals are leaving due to ethical concerns over age and identity verification.

In order for covered entities to make an attempt to comply, professionals are being forced to modify our computer operating systems *causing angst among engineers and programmers because of their professional ethics.* I myself would have difficulty taking many contracts available to me due to these laws.

The Linux Operating System is developed openly so its authors are well known. Linux Weekly News reports that the individual who added the birth date field to its login database has suffered harassment including death threats.

When people in other professions change jobs, leave the district, leave the state, retire early, change fields, or merge their practice into a larger entity, I ask these educators, administrators, healthcare professionals, and technicians about their motivation. These people express ethical concerns, liability concerns, complexity concerns, and burnout over complying with regulations regarding children. These conversations include people who were the only, or among the only people in the State of Vermont serving in their domain of expertise. This trend is exacerbated by Act 63. The fact is that professionals are human beings who are already motivated to protect children.

CONCLUSION

In my opinion the correct course is not for our society to regulate an individual's ability to read, write, and associate, but rather for our society to dissolve the companies which are known to be bad actors.

This year, as the various age verification laws have come online, I have not heard a single anecdote from the parents in my community about a minor who has benefited from age assurance methods or identity verification. On the other hand, I have heard a constant string of stories from parents, teens, and adults about harm done. They are being cut off from their accumulated body of work, from their media, photos, artwork, writing, software, correspondence, publications, subscriptions, their contacts, their support networks, their employers, and ultimately their ability to communicate and operate in their society. It is frustrating for minors, for their parents, and for everyone else. I will conclude with some food for thought: I calculate that the average age of the five founders

of the three major computer systems (Apple, Linux, and Microsoft) was 22 years old at the time the of foundation, and these people had been working toward these systems for several years, starting in their teens. I think that we forget that human development is still on the same track it has always been on and that all people, including minors under the protection of their guardians, do deserve the right to read, write, and associate without regulations like Act 63 actively interfering.

Act 63 ends with the ironic statement, "It is the intent of the General Assembly that nothing in this sub-chapter may be construed to infringe on the existing rights and freedoms of covered minors." Speaking as a parent of three I have to say that this is stunningly false.

Please do not misconstrue any of this report to be malicious to any person or group of Vermonters. I have found, without exception, that the Vermonters I have talked to in my communities, including minors, their parents, people in the engineering, medical, education, journalism, teaching, counseling, administration, and other professions, as well as the school district administration, staff, technology professionals, principles, teachers, and the board, as well as our state and local lawmakers act kindly, patiently, and without malice toward me and my family. I am thankful for their service to our community. These people share or understand my concerns, and they repeatedly and very kindly express their empathy. They are among those who are most keenly suffering under the issues I have mentioned in my report, which can seem impossible to rectify, and this is a strain on their mental health. I believe that the AGO can have a major positive and productive impact on these people and on Vermont society in general with their rule-making by adopting my recommendations.

Bambara, Anthony

Subject: Subject: MAMA Comments on Vermont Age-Appropriate Design Code Rulemaking

From: LaVita Tuff <lavita@wearemama.org>
Sent: Friday, October 2, 2026 4:51 PM
To: AGO - Rulemaking <AGO.Rulemaking@vermont.gov>
Subject: Subject: MAMA Comments on Vermont Age-Appropriate Design Code Rulemaking

Some people who received this message don't often get email from lavita@wearemama.org. Learn why this is important

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Dear Attorney General's Office,

On behalf of Mothers Against Media Addiction (MAMA), please find attached our comments on the implementation of Vermont's Age-Appropriate Design Code (Act 63).

We appreciate the opportunity to provide input and share the perspective of parents and families as the Office develops these important rules.

Thank you for your consideration.

--
Best wishes,
LaVita Tuff, J.D., M.U.R.P.
Policy Director
lavita@wearemama.org
MAMA – Mothers Against Media Addiction

MAMA
Mothers Against
Media Addiction

October 2, 2026

Office of the Vermont Attorney General
Re: Vermont Age-Appropriate Design Code Rulemaking, Act 63

Dear Attorney General Clark:

Mothers Against Media Addiction (MAMA) appreciates the opportunity to comment on implementation of Vermont's Age-Appropriate Design Code (AADC), Act 63.

MAMA is a grassroots movement of parents and allies working toward a world where real-life experiences and interactions remain at the heart of a healthy childhood. We believe technology should serve children and families, not the other way around. Products used by children should be designed with their safety, privacy, and developmental needs in mind from the start.

As Vermont develops rules addressing compulsive use and practices that impair autonomy, decision-making, or choice, MAMA encourages the Attorney General to prioritize the following:

1. **Evaluate how design actually affects children.** Rules should focus on how features function and their reasonably foreseeable effects, not how companies describe them. Relevant practices include autoplay, infinite scroll, streaks, variable rewards, engagement-driven notifications, algorithmic recommendations, social validation features, default-on personalization, and unnecessary friction that makes it harder to disengage. The cumulative effect of these features should also be considered.
2. **Apply protections based on function and risk.** Child protections should not depend on whether a company labels its product social media, gaming, entertainment, education, or AI. Relevant practices should be addressed wherever they appear, including social media, gaming, streaming, messaging, AI chatbots and companions, generative AI, educational technology, connected toys, and emerging technologies.
3. **Address the data practices behind engagement.** The rules should consider behavioral profiling, personalized recommendation systems, engagement optimization, dark patterns, and other practices that use information about children to shape their behavior or increase engagement. MAMA supports data minimization, purpose limitation, and strong restrictions on unnecessary secondary uses of children's information.
4. **Account for AI and emerging technologies.** AI chatbots, companions, AI-enabled toys, and generative AI raise additional concerns about personalization, persuasion, emotional attachment, and repeated engagement. Rules should consider whether AI systems simulate relationships,

encourage emotional dependency or continued interaction, or use information learned from a child to personalize future interactions.

5. **Do not create an educational loophole.** An educational purpose should not exempt a product's design or data practices from scrutiny. This is particularly important when schools require children to use technology and students cannot simply choose to disengage. Educational technology should be held to strong standards for safety, privacy, data minimization, and responsible design.
6. **Keep the physical-product exclusion narrow.** A digital service should not escape scrutiny simply because it is embedded in or connected to a physical product. If a connected toy or other product profiles children, provides personalized content, incorporates engagement-maximizing features, collects unnecessary information, or offers an AI companion or similar interactive experience, those digital functions should be evaluated on their own merits.
7. **Make safety and privacy the default.** Children should receive strong privacy protections by default, and businesses should minimize the information they collect and use. Higher-risk and AI-enabled products should be subject to appropriate evaluation, independent testing and oversight, incident reporting, and reassessment when significant features change. Age assurance should also be implemented in ways that minimize the collection and retention of personal information.
8. **Do not shift responsibility onto families.** Transparency, parental controls, consent mechanisms, warnings, and opt-outs can be useful, but they are not substitutes for safe design. Families should not have to navigate complicated settings or continually opt out of engagement-maximizing features to make products safer for their children. Businesses that design and deploy these products are best positioned to address foreseeable risks at the source.

Finally, the Attorney General should consider a child's developmental stage, frequency and duration of use, whether use is voluntary or required, accessibility needs, and the cumulative effects of multiple design and data practices. The appropriate inquiry should be how the product functions as a whole and whether its design foreseeably contributes to compulsive use or impairs a child's autonomy, decision-making, or choice.

Technology will continue to evolve. Vermont's rules should therefore establish durable protections focused on the underlying design practices, data uses, and incentives that create risks for children.

Parents deserve a meaningful voice, but they should not carry the responsibility for making unsafe products safe. **Child safety should be the design default.**

Thank you for the opportunity to provide comments.

Sincerely,

LaVita Tuff, J.D., M.U.R.P.
Policy Director
Mothers Against Media Addiction (MAMA)
WeAreMAMA.org