



NATIONAL
ASSOCIATION OF
ATTORNEYS GENERAL

PRESIDENT

Ellen F. Rosenblum
Oregon
Attorney General

PRESIDENT-ELECT

John Formella
New Hampshire
Attorney General

VICE PRESIDENT

William Tong
Connecticut
Attorney General

IMMEDIATE PAST
PRESIDENT

Dave Yost
Ohio
Attorney General

Brian Kane
Executive Director

1850 M Street NW
12th Floor
Washington, DC 20036
(202) 326-6000
www.naag.org

March 7, 2024

Via Federal eRulemaking Portal

Federal Trade Commission
Office of Secretary April Tabor
600 Pennsylvania Ave NW
Suite CC-5610 (Annex B)
Washington, DC 20580

RE: COPPA Rule Review, Project No. P195404

Comments of the Attorneys General of Oregon, Illinois, Mississippi, Tennessee, Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Indiana, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, South Dakota, Utah, Vermont, Virgin Islands, Virginia, Washington and Wisconsin

Dear Secretary Tabor:

On behalf of the Attorneys General of Oregon, Illinois, Mississippi, Tennessee, Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Indiana, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, South Dakota, Utah, Vermont, Virgin Islands, Virginia, Washington and Wisconsin ("the States"), we submit the following comments as requested by the Federal Trade Commission ("the Commission")¹ on its implementation of the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506 (1998) ("COPPA"), through regulations codified at 16 C.F.R. part 312 (2013) ("the COPPA Rule").

¹ See Children's Online Privacy Protection Rule, 89 Fed. Reg. 2034, 2069 (proposed amendments Jan. 11, 2024) (to be codified at 16 C.F.R. pt. 312).

Under 15 U.S.C. § 6504, State Attorneys General are authorized to bring actions under COPPA as *parens patriae* in order to protect their citizens from harm. As partners with the Commission in ensuring COPPA is enforced and children are protected, the States possess a unique and important perspective on how effective the COPPA Rule has been, the fundamental values and protections it upholds, and what improvements should be made.

Since the COPPA Rule became effective on April 21, 2000, State Attorneys General, on their own and in partnership with the Commission, have pursued actions for violations of the COPPA Rule.²

It has been more than ten years since the COPPA Rule was amended to address the increased use of mobile devices and social networking. The digital landscape is a much different place than it was in 2013. We urge the Commission to update the COPPA Rule to keep pace and give State Attorneys General the tools they need to respond to a digital world rife with risk.

A. Comments to Proposed Revisions to the Rule – Definitions

- 1. Proposed Rule Revision No. 5: “The Commission proposes adding biometric identifiers such as fingerprints, retina and iris patterns, a DNA sequence, and data derived from voice data, gait data, or facial data to the definition of ‘personal information.’ Should the Commission consider including any additional biometric identifier examples to this definition? Are there exceptions to the Rule’s requirements that the Commission should consider applying to biometric data, such as exceptions for biometric data that has been promptly deleted?”**

Yes, the Commission should further revise the definition of “Personal Information” to include biometric data, defined broadly to include genetic information. In addition, the Commission should consider healthcare information and other highly sensitive data to bolster the protection from the profound risk of harm due to the illegal collection this data poses.

Biometric data should be defined broadly to encompass imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings (from which an identifier template such as a faceprint, a minutiae template, or a voiceprint, can be extracted), genetic data, or other unique biological, physical, or behavioral patterns or characteristics, including data generated by any of these data points. For example, not just the fingerprint should be protected, but the mathematical representation of a fingerprint frequently used for scanning devices.

² See Compl., *FTC v. Google LLC and YouTube, LLC*, No. 1:19-cv-02642 (D.D.C. filed Sept. 6, 2019), available at <https://www.ftc.gov/enforcement/cases-proceedings/172-3083/google-llc-youtube-llc>; *New Mexico v. Rovio Entertainment Corp.*, D.N.M., No. 1:21-cv-824 (Aug. 25, 2021); *State of Arizona, et al. v. Meta Platforms, Inc. et al.*, No. 4:23-cv-05448 (2023 N.D. Cal.).

In addition to traditional biometric data points, the Commission should protect healthcare data, defined to capture at minimum keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information. Furthermore, there are inextricably linked sensitive data points that may not only relate to health but also to a child's identity.

Wearable digital health technology has been the subject of several high-profile privacy and data misuse concerns in recent years.³ Rapid advancements in sensor technology have enabled the integration of sensors into a wide range of wearable devices, from fitness trackers to smartwatches—the estimated market for wearable sensors is expected to grow from \$3.55 billion in 2023 to \$10.19 billion in 2033.⁴ The prevalence of the collection and use of this type of data—from using a fingerprint to unlock a device to wearable sensors—has resulted in a heightened risk of abuse and sale of this type of data, data that is often immutable and permanently tied to the individual. While some of the data may not be instantaneously identifiable, when combined with other persistent identifiers such as an IP address or device ID, it may be possible to tie this information to an individual.

The Commission should not consider an exclusion from biometric data for data that is promptly deleted. Considering the highly sensitive nature of this data, excluding it from consideration from COPPA based on whether it has been promptly deleted creates an avenue around the regulation that would not be in children's best interest or align with the purpose of the regulation. For state laws that have a similar carve-out, the carve-out does not apply to minors under 13⁵ and the carve-out does not remove those data points entirely from regulation.⁶ Other protections still apply such as data protection assessment and disclosure requirements.⁷ The mere fact that the data is collected and temporarily held makes it vulnerable to potential cybersecurity attacks or misuse. Considering the high sensitivity of the data and the vulnerability of the regulated population under COPPA, the Commission should not lessen the teeth of the proposed inclusion of biometric protection by allowing any exceptions to the regulation.

2. Proposed Rule Revision No. 6: “The use of avatars generated from a child's image has become popular in online services, such as video games. Should an avatar generated from a child's image constitute ‘personal information’ under the COPPA Rule even if the photograph of the child is not itself uploaded to the site or service and no other

³ See, e.g., Liz Sly, *U.S. Soldiers are Revealing Sensitive and Dangerous Information by Jogging*, Washington Post (Jan. 29, 2018, 5:22 AM), https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html.

⁴ *Wearable Sensors Market Expected to Reach USD 10.19 Billion by 2033 | Impressive CAGR of 12.8%*, Yahoo! Finance (Jan. 29, 2024), <https://finance.yahoo.com/news/wearable-sensors-market-expected-reach-085100298.html#:~:text=New%20York%2C%20Jan.%2029%2C,period%20from%202023%20to%202032>.

⁵ See exemptions under COLO. REV. STAT. § 6-1-1304 (2023).

⁶ 4 COLO. CODE REGS. § 904-3, Rule 6.10(B) (2023).

⁷ See COLO. REV. STAT. § 6-1-1309 (2023).

personal information is collected from the child? If so, are these avatars sufficiently covered under the current COPPA Rule, or are further modifications to the definition required to cover avatars generated from a child's image?"

Yes, the Commission should revise 16 C.F.R. § 312.2 ("§ 312.2") definition of personal information to include the following: "an avatar generated on the child's image and likeness, whether or not a photograph, video or audio file is provided or stored." In 2013, the Commission expanded the Rule's definition of personal information to include "[a] photograph, video or audio file where such file contains a child's image or voice."⁸ We encourage the Commission to further clarify that avatars should be a protected element of personal information. With the prevalence and rise of online services and social media sites, video games, and virtual reality, it is critical to take a forward-looking stance on protecting this information from the potential to be exploited.

With the increased possibility of companies using biometric data to generate an avatar based on a person's likeness, regulations should adapt to consider the privacy and cybersecurity concerns that arise from the potential storage of this data, including the risk that an avatar could be reverse engineered. The traditional forms of avatars are evolving, virtual reality is a growing space and frequently utilizes digital representations of the human user, an avatar, to allow the user to see and interact with virtual reality environments and other users. If the avatars are based on the child's photograph or likeness, regardless of whether the original source is retained, the avatar could be used in the identification of the child, through many different methods including reverse image searches, facial recognition tools, or combining information gleaned from the avatar with other known elements of personal information.

Explicitly identifying the definition of personal information to include avatars modeled with a child's image and likeness allows for clearer disclosures and efficient enforcement against violations for purposes of protecting the children.

3. Proposed Rule Revision No. 7: "The definition of 'personal information' includes a Social Security number. Should the Commission revise this definition to list other government-issued identifiers specifically? If so, what type of identifiers should be included?"

Yes, the Commission should revise the definition of government-issued identifiers to include, at a minimum, passport and passport card numbers, Alien Registration numbers or other identifiers from USCIS, Birth Certificate numbers, any unique identifiers used to access public benefits, State ID card numbers, and student ID numbers. These numbers are highly sensitive, have a high risk if exploited, and should be granted the protection of all other Personal Information under COPPA. A parent should have the right to review with their child before giving any of these identifiers to a third-party, particularly when the result of misuse or exploitation could have a serious lasting effect on a child's life.

⁸ See "Audio File Exception," 89 Fed. Reg. at 2058.

4. Proposed Rule Revision No. 8: “The definition of ‘personal information’ includes ‘information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in [the Rule’s definition of ‘personal information’].’ Does the phrase ‘concerning the child or parents of that child’ require further clarification?”

Yes, the phrase “concerning the child or parents of that child” does require further clarification and the State Attorney Generals propose clarifying the definition, while avoiding the narrowing of the definition by including the additional language below in bold:

The definition of “personal information” includes “information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in [the Rule’s definition of ‘personal information’], **or which may otherwise be linked or reasonably linkable to personal information of the child.**”

The Commission has identified the risk of children’s personal information being exposed in [a] previous settlement.⁹ For example, if companies are linking profiles of both parent and child, then the aggregated information of both profiles can indirectly expose the child’s personal information such as their home address even when it was not originally submitted by the child to invoke COPPA.

Further clarification is necessary in situations where a child and parent separately provide information during the account creation process. For example, as detailed in a previous Commission settlement, the company had the user input data before requiring users under the age of 13 to involve their parent. The information entered by the child before being prompted to involve their parent, can be aggregated with the data entered by their parent, triggering COPPA protections.¹⁰ This remains a threat even if the personal information is input for an account creation process that is never completed.

The benefit of this clarification would prevent situations the Commission has referenced in past settlements by closing this gap in COPPA to directly protect children’s online privacy.

5. Proposed Rule Revision No. 9: “Certain commenters recommended modifications to the “support for the internal operations of the website or online service” definition, including to limit personalization to “user-driven” actions and to exclude methods

⁹ Lesley Fair, *Vtech Settlement Cautions Companies to Keep COPPA-Covered Data Secure*, FTC Business Blog (Jan. 8, 2018), <https://www.ftc.gov/business-guidance/blog/2018/01/vtech-settlement-cautions-companies-keep-coppa-covered-data-secure>.

¹⁰ Lesley Fair, *\$20 Million FTC Settlement Addresses Microsoft Xbox Illegal Collection of Kids’ Data: A Game Changer for COPPA Compliance*, FTC Business Blog (Jun. 5, 2023), [\\$20 million FTC settlement addresses Microsoft Xbox illegal collection of kids’ data: A game changer for COPPA compliance | Federal Trade Commission](#).

designed to maximize user engagement. Under what circumstances would personalization be considered “user-driven” versus personalization driven by an operator? How do operators use persistent identifiers, as defined by the COPPA Rule, to maximize user engagement with a website or online service?”

The States support modifying the definition of “[s]upport for the internal operations of the website or online service” to limit personalization to “user-driven” actions and exclude operator methods that are intended to maximize user engagement. This is cohesive with the core purpose of the functions defined under § 312.2 and speaks directly to protecting children who may be particularly vulnerable to being influenced by suggested content.

User-driven personalization could be considered tools enabling users to customize the experience to meet their needs by configuring layout, content, or system functionality. Customization could involve moving items around an interface to reflect the users’ priorities or altering factors related to the visual design of an interface, such as changes to the accessibility functions. Creations of playlists, subscriptions, and comments sections are all forms of the user-driven experience.¹¹

In contrast, operators may utilize personalization tactically—using an algorithm to automate suggested products, shows and videos. These recommendations are based on data collected from what users search, purchase and watch, and these methods could be used to influence and manipulate what children watch and interact with.

Exceptions to the collection of persistent identifiers should be construed as narrowly as possible, particularly when there has been a history of noncompliance. A study published in 2019 tested 5,855 Android apps that were directed to children and found that more than half appeared to be violating COPPA.¹² In fact, Apple requires that no persistent identifiers can even be collected from children’s apps, demonstrating that they are not vital to the support and operation of applications. Based on the high likelihood of abuse and the potential for persistent identifiers to be used to influence children by third parties, we recommend the Commission consider, at a minimum, limiting permissible personalization to “user-driven” actions.

6. Proposed Rule Revision No. 10: “Operators can collect persistent identifiers for contextual advertising purposes without parental consent so long as they do not also collect other personal information. Given the sophistication of contextual advertising today, including that personal information collected from users may be used to enable

¹¹ Garrett A. Johnson, et al., *COPPAcalypse? The YouTube Settlement’s Impact on Kids Content*, 1, (May 1, 2023, last revised Jan. 2, 2024), <https://ssrn.com/abstract=4430334>.

¹² *Protecting Kids Online: Internet Privacy and Manipulative Marketing*: Hearing on S. 253 Before the S. Comm. on Consumer Protection, Product Safety, and Data Security, 117th Cong. 3 (2021) (*Testimony of Serge Egelman, Ph.D., Research Dir., International Computer Science Institute*).
<https://www.commerce.senate.gov/services/files/ODC78E9D-88B2-4D54-8F4A-AE7B4C7D0EF6>.

companies to target even contextual advertising to some extent, should the Commission consider changes to the Rule's treatment of contextual advertising?"

Yes, the Commission should consider changes to the Rule's treatment of contextual advertising. Currently, COPPA allows operators to collect persistent identifiers for contextual advertising purposes without parental consent so long as they do not also collect other personal information. Although COPPA permits "contextual advertising," that term is not defined within the text of the law itself. We recommend that the Commission provide a specific definition for "contextual advertising" that (1) limits the scope of an advertiser's ability to collect defined personal identifiable information ("PII") through artificial intelligence ("AI") for advertisement targeting purposes; and (2) prohibits collection of browser histories, IP addresses, and locations data, all of which allow advertisers to operate in a targeted fashion. By utilizing current behavioral tracking mechanisms, advertisers are now providing children with a greater individualized experience without parental consent. With a modification to COPPA's definition of "contextual advertising" that bans post-2013 behavioral tracking practices, the Commission can return COPPA's "contextual advertising" provision to its original intended purposes, which is to allow advertisers to provide children with generalized advertisements that are aligned with the theme of a specific visited webpage, rather than children's internet search habits.

In the early and mid-2000s, contextual advertising was considered the most privacy-friendly method for online advertising. It did not rely on cookies or other personal identifiers. It simply provided advertising to individuals based on the environment in which an ad appears. For example, if someone is browsing the internet in preparation of a hiking trip and visits a website that sells hiking gear, the visitor may be provided with advertisements for hiking boots. These advertisements are directly in-line with the items provided for on the visited webpage, and do not use specific identifiers to target the consumer. Rather, the advertisers are recommending items for purchase based on the environment of the website, which in this case would be hiking. It is this conduct that is reflected in the 2009 Commission Report's definition of "contextual advertising."¹³ This definition is outdated.

Technology has rapidly evolved since 2009 making obsolete the definition found in the 2009 Commission Report. Today, contextual advertisers utilize AI, like Verge Group's Moments.AI, a real-time contextual advertising service, to track browser and page-level data, device data, IP address, and location data to create models of potential users for an enhanced advertising experience. GumGum is a contextual intelligence platform that enables brands to engage customers with sought after products in their current moment and environment through utilizing AI and deep-learning algorithms that analyze a

¹³ FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising, Behavioral Advertising: Tracking, Targeting, & Technology, (Feb. 2009), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf> (where the 2009 FTC Report defined contextual advertising as "advertising based on a consumer's current visit to a single web page or a single search query that involves no retention of data about the consumer's online activities beyond that necessary for the immediate delivery of an ad or search result.").

customer's context, including text, speech, imagery, and geolocation. Amazon's "recommendation system" is also a form of contextual advertising, which displays products that are similar to or are associated with the items that customers are viewing or are in their shopping carts. As for children, this means that advertisers, without parental consent, are actively tracking children's browser history and habits to provide them with specific advertisements. Consequently, children, without a parent's knowledge, could be lured into making purchases or providing data without knowledge, according to Samuel Levine, Director, Commission's Bureau of Consumer Protection.¹⁴ Mr. Levine also noted that contextual advertising in digital environments puts children in a vulnerable position to succumb to fraud.¹⁵

AI has moved contextual advertising from basic keyword searches to a much deeper and more accurate understanding of digital content, which significantly improves the effectiveness of contextual targeting with greater precision. This practice is referred to as "contextual 2.0" in the advertising sector. This is only the beginning of AI's impact on contextual advertising and contextual practices are likely to become even more tailored with advanced machine learning models. The progression and advancement of contextual advertising practices through AI warrants an amendment to COPPA's vague language that permits non-defined contextual advertising. In sum, a clearer definition as to what constitutes "contextual advertising" and what types of data can be used may help address Commission concerns. This would also curb AI that is shifting contextual advertising away from its intended purpose.

- 7. Proposed Rule Revision No. 11: "With regard to the definition of 'website or online service directed to children,' the Commission would like to obtain additional comment on whether it should provide an exemption for operators from being deemed a child-directed website or online service if such operators undertake an analysis of their audience composition and determine no more than a specific percentage of its users are likely to be children under 13.**
 - A. Should the COPPA Rule offer an exemption or other incentive to encourage operators to conduct an analysis of their user bases?**
 - b. If the COPPA Rule should include such an exemption or other incentive, what are the reliable means by which operators can determine the likely ages of their sites' or services' users?**
 - c. As part of this exemption or incentive, should the COPPA Rule identify which means operators must utilize to determine the likely ages of their users? If so, how should the COPPA Rule identify such means?**

¹⁴ Staff Perspective, *Protecting Kids from Stealth Advertising in Digital Media*, FTC, (Sept. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p214505kidsadvertisingstaffperspective092023.pdf (last accessed on Feb. 15, 2024).

¹⁵ *Id.*

- d. If the COPPA Rule should include such an exemption or other incentive, what should be the appropriate percentage of users to qualify for this exemption or incentive?**
- e. Would such an exemption be inconsistent with the COPPA Rule's multi-factor test for determining whether a website or online service, or a portion thereof, is directed to children?"**

The States do not believe that any exemption should be provided based on audience or user composition. The personal information currently covered by COPPA represents sensitive, identifying data. 16 C.F.R. § 312.2. COPPA serves an important reminder to website operators of both the private nature and risk of harm of these categories. In considering exemptions, policymakers must remember that potential harm is present on an individual basis—the amount of children who use a platform do not affect how sensitive or worthy of protection the data on that platform could be. Indeed, “general purpose” websites not explicitly directed at children provide much broader opportunities for children and adults to interact, more opportunities for the disclosure of personal information, and broader opportunities for harm.

Instead of exemptions, we encourage operators to decrease the overall collection of personal information and decline to collect information from anyone identified to be under 13 unless such collection meets COPPA requirements. A website that does not collect or store any personal information would have no need for an exception, and a website which does collect such information must be held to a high standard of conduct without exception.

Finally, any attempt to incentivize operators to perform user-base analysis must not in itself result in greater personal information collection. An attempt to gain an exemption from COPPA may result in greater harvesting of adult user data, an unintended but troubling consequence. We feel that COPPA penalties for the mishandling of children's personal information should be crafted to provide sufficient encouragement for proactive analysis and compliance.

B. Comments to Proposed Revisions to the Rule – Parental Consent

- 1. Proposed Rule Revision No. 13: “Can platforms play a role in establishing consent mechanisms to enable app developers or other websites or online services to obtain verifiable parental consent? If so, what benefits would a platform-based common consent mechanism offer operators and parents? What steps can the Commission take to encourage the development of platform-based consent mechanisms?”**

The States believe that industry partners, platforms, and other non-government entities can play a role in establishing consent mechanisms to enable operators to obtain verifiable consent.

Taking measures to centralize the process for obtaining verifiable parental consent (“VPC”) through platform or device based common consent mechanisms can help reduce the burden on parents by limiting the number of times a parent must engage in the process of providing VPC. Additionally, given that many VPC methods require the provision of sensitive, identifying data—such as government issued IDs, biometric data, and payment card information—platform or device based common consent mechanisms could reduce the number of times a parent would need to provide such sensitive information.¹⁶ Further, should VPC be conducted on platforms such as Google or Apple, it is possible that the process would build on those already in place and utilized by parents (*i.e.*, parents may receive notifications when a child or teen attempts to make a purchase; the platforms already have optional services through which a parent can manage or block apps from being downloaded). VPC providers should be subject to the same requirements as their clients are under COPPA.

A platform or device based common consent mechanism may reduce the burden such costs pose for smaller and midsized developers.¹⁷ However, we would caution against any changes that would relieve operators of the responsibility of having age-appropriate features and protections in place.

In order to develop platform or device based consent mechanisms, the Commission could partner with a developer to create a government-approved identification and age-verification application. The UK has already implemented a single sign-on system which third parties can implement for age and identity verification.¹⁸ The Commission may choose to either partner directly with a developer and create its own app, or offer certification to third-party apps that they meet certain security and legal requirements.

Alternatively, the Commission could explicitly allow the use of certain age verification tools, to be periodically approved by the Commission, which could provide a presumption of compliance as to VPC-specific requirements, or implement caps to liability. This could mirror the incentives present in the SAFETY Act.¹⁹

Finally, the Commission could look to the 2023 presidential National Cybersecurity Strategy²⁰ for guidance, particularly Pillars Three and Four, which serve to shape market forces and provide incentives. These include research and development, labeling requirements, and liability shifting provisions. Of particular interest may be Strategic Objective 4.5: Support Development of a Digital Identity Ecosystem,²¹ which focuses on

¹⁶ See *THE STATE OF PLAY: Is Verifiable Parental Consent Fit for Purpose?*, Future of Privacy Forum (Jun. 2023), 19-20, <https://fpf.org/wp-content/uploads/2023/06/FPF-VPC-White-Paper-06-02-23-final2.pdf>.

¹⁷ See *Id.*, at 13.

¹⁸ See Let Users Sign in and Prove their Identity to Use Your Service, <https://www.sign-in.service.gov.uk/>.

¹⁹ Frequently Asked Questions, Homeland Security, Science and Technology, <https://www.safetyact.gov/lit/f/ags>.

²⁰ OFFICE OF THE NATIONAL CYBER DIRECTOR, NATIONAL CYBERSECURITY STRATEGY (Mar. 2023), <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.

²¹ See *Id.*, at 30.

creating a secure, convenient, and transparent identity management and verification ecosystem.

2. Proposed Rule Revision No. 14: “To effectuate § 312.5(a)(2), which requires operators to give the parent the option to consent to the collection and use of the child’s personal information without consenting to disclosure of the child’s personal information to third parties, the Commission proposes requiring operators to obtain separate verifiable parental consent prior to disclosing a child’s personal information, unless such disclosure is integral to the nature of the website or online service. Should the Commission implement such a requirement?”

Yes, the Commission should implement the requirement for separate verifiable consent prior to disclosing a child’s personal information. Separate verifiable consent is an effective measure to protect children’s personal information. The States agree with the Commission that the verifiable parental consent requirement is a fundamental component of the COPPA Rule’s ability to protect children’s privacy. Like the Commission, States are concerned about the disclosure of personal information collected from children. The current rule under 16 C.F.R. § 312.5(a)(2) required operators to give parents an option to consent to child personal information collection, use, or disclosure without consenting to disclosure of the parents’ own personal information. The proposed new rule requirement heightens the protection of children’s personal information and allows parents to consent to collection without consenting to disclosure. Separate parental consent requirements for both collection and disclosure of children’s personal information will heighten child privacy. It will also avoid parental confusion by preventing parents from incorrectly assuming that collection, use, and disclosure are “bundled” together. The new proposed rule works to allow parents to control who obtains their child’s information and provides an avenue for parents to further protect their child’s personal information.

“Should the consent mechanism for disclosure be offered at a different time and/or place than the mechanism for the underlying collection and use? Is the exception for disclosures that are integral to the nature of the website or online service clear, or should the Commission clarify which disclosures are integral? Should the Rule require operators to state which disclosures are integral to the nature of website or online service?”

Yes, the consent mechanism for disclosure should be offered at a different time and/or place than the mechanism for underlying collection. The goal for the new proposed rule is to increase the protection of children’s personal information. Without separating the consent mechanisms, parents may believe they are only consenting to collection when they are really consenting to both collection and disclosure. Offering a different time or place to consent to disclosure eases any potential for user confusion. Separation provides parents a way to easily choose whether they consent to disclosure of their child’s information. Parents will first choose to consent to the collection of their child’s personal information. Once a parent consents to the collection of their child’s information, parents can then

choose to consent to the disclosure of their child's information. Separating the consent mechanisms allows parents to make an informed decision and protect their child's personal information. It is unlikely that parents will find this two-step approach confusing or burdensome, since consumers have become more familiar with similar processes like two-factor authentication in recent years.

No, the Commission should consider clarifying what disclosures are integral to the nature of a website or service. "Integral" may carry very different meanings depending on what side of a transaction one is found. From the perspective of a consumer, "integral" may include the services necessary to effectuate the transaction—for example, a third-party payment processor or mailing service. On the other hand, a business operating a website may consider goals such as product development, research, marketing, and even targeted advertising to be "integral" to their service. Because of the potential for confusion, the Commission should define "integral" or use a different term that more clearly illustrates the meaning. And because children's data is particularly sensitive, we believe that any definition of "integral" should err on the side of greater protection and should come from the perspective of the parent. One proposed definition could be—*the minimum disclosure necessary to effectuate the transaction, as reasonably expected by the consumer/parent*. Further, the Commission should include in any definition what is not contemplated in the definition: for example, *"Integral" does not include research & development, marketing, or targeted advertising; "Integral" does not include business functions or goals outside the explicit transaction between the operator and the parent*. Finally, the Commission should explicitly state when the data sharing ends. Once the explicit purpose is fulfilled, data should not be retained or used for any other purpose by the operator or third party.

Yes, operators should be required to state which disclosures are integral to the nature of their website or online service. This information should be understandable and accessible. Colorado's 2021 Privacy Act contains language that the Commission may find useful regarding operators and disclosures. Language from Colorado's 2021 Privacy Act is instructive: Communications must be "provided in a readable format on all devices through which consumer normally or regularly interact with the controller, including on smaller screens and through mobile applications, if applicable."²² The States suggest that operators identify which disclosures are integral to the nature of their website or online service in a format that is readable on all devices through which the consumer interacts with the controller.

- 3. Proposed Rule Revision No. 15: "As noted in Part IV.C.3.c., the Commission proposes to modify § 312.5(c)(4) to prohibit operators from utilizing this exception to encourage or prompt use of a website or online service. Are there other engagement techniques the Rule should address? If so, what section of the Rule should address them? What types of personal information do operators use when utilizing engagement techniques? Additionally, should the Rule differentiate between techniques used solely to promote a child's engagement with the website or online service and those techniques that**

²² 4 COLO. CODE REGS. 904-3, Rule 3.01(5).

provide other functions, such as to personalize the child’s experience on the website or online service? If so, how should the Rule differentiate between those techniques?”

We support the Commission’s proposal to prohibit operators from abusing the multiple-contact exception in 16 C.F.R. § 312.5(c)(4) with engagement-maximizing push notifications. By design, push notifications serve to draw children back onto a platform when they were otherwise engaged in a different activity. Children currently receive an enormous volume of push notifications; in a week-long study of 203 11- to 17-year-olds, the median participant received 237 notifications per day.²³ This deluge threatens to disrupt children’s sleep, distract from their education, and detract from family activities and personal hobbies. Operators should not be permitted to promote further engagement with their platforms via push notifications absent prior parental consent.

Additionally, systems can leverage data on a user’s behavior to recommend further content to the user. This can sometimes be innocuous but also carries significant risks. We urge the Commission to empower parents to elect the non-use of their child’s personal user data to feed into an algorithm-driven content personalization system. This feature should be included during the verifiable consent period.

To address these risks, the Commission should clarify the proper scope of the Rule’s internal operations exception. That exception permits operators to collect persistent identifiers without parental consent for the “purpose of providing support for the internal operations of the Web site or online service.” 16 C.F.R. § 312.5(c)(7). The Commission has interpreted this to allow the collection of children’s persistent identifiers to “personalize content.”²⁴ The Commission should clarify that while the internal operations exception permits user driven personalization, it does not allow operators to implement algorithm-driven content personalization without parental consent.

The Commission has explained that the personalization envisioned by the Rule pertains to “user driven preferences, such as game scores, or character choices in virtual worlds.”²⁵ But, algorithm-driven personalization is *not* user-driven. Instead, it leverages subtle observations about a child’s engagement and behaviors—how long they watch a video, which kinds of games they click on, or how long they hover over a part of a website—to recommend further content for the child to engage with. At bottom, extended engagement is the primary purpose of these personalization algorithms²⁶—steering children to stay online longer, regardless of whether they have any affirmative desire to do so.

²³ Jenny S. Radesky et al., *Constant Companion: A Week in the Life of a Young Person’s Smartphone Use*, Common Sense Media, 6, (Sept. 26, 2023), <https://www.common Sense Media.org/research/constant-companion-a-week-in-the-life-of-a-young-persons-smartphone-use>.

²⁴ Complying with COPPA: Frequently Asked Questions, FTC Business Guidance Resources, J-5, <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>.

²⁵ *Id.* at I-8.

²⁶ Arvind Narayanan, *Understanding Social Media Recommendation Algorithms*, 18, (Mar. 9, 2023), <https://academiccommons.columbia.edu/doi/10.7916/khdk-m460>.

Further clarity is important in part because the current Rule does not ensure sufficient transparency for parents. The privacy policies of many child-directed websites suggest—without clearly and directly disclosing—the use of algorithm-driven content personalization. For example, the Walt Disney Company’s Children’s Online Privacy Policy states that children’s information may be collected to “customize content and improve our sites and applications.”²⁷ Similarly, the privacy policy of FunBrain (a popular children’s game site) states that the company “may use your personal information to tailor the content, programming, services, and applications that we provide to meet your needs and interests.”²⁸ These kinds of general disclosures do not adequately apprise parents of how, and why, their children’s data are being used.

4. Proposed Rule Revision No. 16: “The Commission proposes to include a parental consent exception to permit schools, State educational agencies, and local educational agencies to authorize the collection, use, and disclosure of personal information from students younger than 13 where the data is used for a school-authorized education purpose and no other commercial purpose. What types of services should be covered under a ‘school-authorized education purpose’? For example, should this include services used to conduct activities not directly related to teaching, such as services used to ensure the safety of students or schools?”

We recommend that the Commission consider relevant definitions in the Oregon Student Information Protection Act, the California Student Online Personal Information Protection Act and the Connecticut’s Student Data Privacy Act. These statutes, which regulate certain practices of education technology providers, offer guidance on the scope of services covered by the term “school-authorized education purpose.”

According to the Oregon Student Information Protection Act, “Kindergarten through grade 12 school purposes” includes activities that (a) are directed by, or that customarily take place at the direction of, a kindergarten through grade 12 school, teacher, school district, or education service district; (b) aid in the administration of school activities, including instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents; or (c) are primarily for the use and benefit of the school.²⁹

Likewise, the California Student Online Personal Information Protection Act defines “K–12 school purposes” as “purposes that customarily take place at the direction of the K–12 school, teacher, or school district, or aid in the administration of school activities, including, but not limited to, instruction in the classroom or at home, administrative

²⁷ Children’s Privacy Policy, <https://privacy.thewaltdisneycompany.com/en/for-parents/childrens-online-privacy-policy/> (last visited Feb. 20, 2024).

²⁸ Privacy Policy, <https://www.funbrain.com/privacy-policy> (last visited Feb. 20, 2024).

²⁹ OR. REV. STAT. § 336.184(2)(b)(A)–(C) (2015).

activities, and collaboration between students, school personnel, or parents, or are for the use and benefit of the school.”³⁰

Connecticut’s Student Data Privacy Act, which applies to any situation in which school districts, school leaders and educators use educational technology that captures or accesses personal student information, records or data, also warrants consideration.³¹ Connecticut’s statute defines “school purposes” as “purposes that customarily take place at the direction of a teacher or a local or regional board of education, or aid in the administration of school activities, including, but not limited to, instruction in the classroom, administrative activities and collaboration among students, school personnel or parents or legal guardians of students.”³²

These definitions, when considered together, offer a comprehensive framework for determining the eligibility of services under the proposed parental consent exception. They highlight the importance of activities that are directly related to education, administration, collaboration, and the overall well-being of students within the educational environment.

We believe that adopting a similar approach to what constitutes “school-authorized education purpose” in the Rule will ensure clarity and consistency in determining the scope of services eligible for the proposed exception while maintaining a focus on safeguarding student privacy.

C. Comments to Proposed Revisions to the Rule - Prohibition Against Conditioning a Child’s Participation on Collection of Personal Information

1. Proposed Rule Revision No. 17: “COPPA and § 312.7 of the Rule prohibit operators from conditioning a child’s participation in an activity on disclosing more personal information than is reasonably necessary to participate in such activity.”

“b. Should the Commission specify whether disclosures for particular purposes are reasonably necessary or not reasonably necessary in a particular context? If so, for which purposes and in which contexts?”

The States urge the Commission to maintain the flexible approach in 16 C.F.R. § 312.7 (“§ 312.7”). Assessing whether specific data practices meet the criterion of being “reasonably necessary” requires a detailed, fact-specific analysis. Moreover, the technology landscape is rapidly evolving and situations that may be unimaginable today could become commonplace within a few years. As a result, creating a bright line rule could have unintended effects.

³⁰ CAL. BUS. & PROF. § 22584(j) (2015).

³¹ Student Data Privacy, Resources for Connecticut Public Schools, Connecticut State Department of Administrative Services, <https://portal.ct.gov/DAS/CTEdTech/Commission-for-Educational-Technology/Initiatives/Student-Data-Privacy#boards>.

³² CONN. GEN. STAT. § 10-234aa (2022).

The language currently in § 312.7 of the Rule is consistent with the flexible approach taken in state comprehensive consumer privacy laws.

The laws currently in effect in Colorado, Connecticut, Virginia, and Utah emphasize that personal data processing should be, “adequate, relevant, and limited to what is necessary” for its intended purposes.³³ That framework has been adopted in 8 additional state laws that take effect over the next three years.³⁴ Similarly, the California Consumer Privacy Act employs a “reasonably necessary and proportionate” standard, particularly concerning the collection, use, retention, and sharing of personal information.³⁵ This formulation places guardrails around businesses’ use of personal information without being overly proscriptive, an acknowledgement that the laws cannot account for every possible scenario in this space. Therefore, we believe that it is a sound approach for the Commission to continue to follow in § 312.7. That said, we believe that additional guidance may be beneficial and suggest that the Commission delineate factors for operators to consider in evaluating whether a disclosure is reasonably necessary. We also encourage the Commission to provide illustrative examples. For instance, if an app is designed to tailor a child’s learning experience based on their grade level or age, it would be reasonably necessary for a child to disclose their birth year and grade level but not their precise geolocation. The child might need to also disclose their school affiliation/email address if the app has agreements with certain school districts that allow a child access to additional content. In contrast, the child would not need to provide a Social Security number, gender, or photograph. Businesses should always carefully consider the need to obtain certain data points and thoroughly evaluate factors such as the purpose of the data, potential risks to the child’s privacy, and available alternatives.

³³ Colorado Privacy Act, S.B. 21-190. (2021). https://coag.gov/app/uploads/2022/01/SB-21-190-CPA_Final.pdf; Connecticut Data Privacy Act, S.B. 6. Public Act No. 22-15. (2023). (effective date). <https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-ROOSB-00006-PA.PDF>; Utah Consumer Privacy Act, S.B. 227. (2023). (effective date). <https://le.utah.gov/~2022/bills/static/SB0227.html>; Virginia Consumer Data Protection Act, §59.1-575. (2021) <https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/>.

³⁴ [DE LEGIS 197 \(2023\)](#), [2023, Delaware Laws Ch. 197](#) (H.B. 154); [Indiana Senate Bill 5 \(2023\)](#); 2023 [Iowa Senate File No. 262](#), [Iowa Ninetieth General Assembly, 2023 Session](#); [MT LEGIS 681 \(2023\)](#), [2023 Montana Laws Ch. 681](#) (S.B. 384); [2022 New Jersey Senate Bill No. 332](#), New Jersey Two Hundred Twentieth Legislature, Second annual Session; [ORS 646A.570 to 646A.589](#), [Oregon SB 619](#); 2023 [Texas House Bill No. 4518](#), [Texas Eighty-Eighth Legislature](#); [2023 Tenn. Pub. Acts Ch. No. 408 §§ 47-18-3204\(a\)\(1\)](#), available at <https://publications.tnsosfiles.com/acts/113/pub/pc0408.pdf>.

³⁵ California Consumer Privacy Act, as amended by the California Privacy Rights Act, Cal. Civil Code, § 1798.100, subdivision (c). https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

Similar language also appears in the bipartisan draft federal privacy bill, the American Data Privacy and Protection Act. See American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022), <https://www.congress.gov/bill/117th-congress/house-bill/8152/text#tocH2505DD6E75214E79A8CB1B2EOA7EDDCD>.

By facilitating a structured set of considerations, the Commission can facilitate a more transparent and informed decision-making process for businesses, thereby promoting greater alignment with privacy objectives and enhancing consumer protection measures.

“c. Given that operators must provide notice and seek verifiable parental consent before collecting personal information, to what extent should the Commission consider the information practices disclosed to the parent in assessing whether information collection is reasonably necessary?”

The States believe that the Commission should review the information practices disclosed to the parent, but such disclosures should not be determinative in deciding whether the collection of information from the child was reasonably necessary. The proposed revisions to the direct notice and general notice requirements in 16 C.F.R. § 312.4 of the Rule will certainly aid parents in evaluating whether to give consent. However, an operator stating what information it collects and giving some reason for that collection, does not mean that the collection is, in fact, reasonably necessary for use of that product or service.

The Commission’s proposal to augment 16 C.F.R. § 312.4(c)(1)(iii) by including “how the operator intends to use such information” represents a significant step toward enhancing parental understanding and decision-making regarding consent to their child’s personal information collection.

Expanding on this, the States propose that the Commission should go a step further by considering requiring operators to disclose the purpose of use for each item of information if it’s intended to be shared with a third party. For instance, if an operator plans to collect a child’s first name, geolocation, and address, they should be obligated to disclose the specific purpose for why the name, geolocation, and address, individually, will be shared with third parties. This would provide parents with a more comprehensive understanding of how their child’s data may be utilized beyond the initial collection, enabling them to make more informed decisions regarding consent.

To provide more comprehensive guidance, the Commission may consider adopting language similar to that of Colorado’s Privacy Law.³⁶ Colorado’s Privacy Law mandates that notices include the purposes for which the categories of personal data are processed. This addition would ensure that not only are the types of collected personal information disclosed to parents but also the specific reasons or intentions behind processing each category of individual data.

By implementing such measures, the Commission can ensure that parents are equipped with the necessary information to assess the appropriateness of data collection

³⁶ Colorado: Analyzing Controller Obligations Under the Colorado Privacy Act, One Trust Data Guidance (Sept. 2021), <https://www.dataguidance.com/opinion/colorado-analysing-controller-obligations-under>.

practices involving their children, thereby fostering a safer and more transparent online environment for minors.

2. Proposed Rule Revision No. 18: “The Commission is considering adding new language to address the meaning of ‘activity,’ as that term is used in § 312.7. Specifically, the Commission is considering including language in § 312.7 to provide that an ‘activity’ means ‘any activity offered by a website or online service, whether that activity is a subset or component of the website or online service or is the entirety of the website or online service.’ Should the Commission make this modification to the Rule? Is this modification necessary in light of the breadth of the plain meaning of the term ‘activity’?”

After careful consideration, we would suggest maintaining the current definition of “activity” in § 312.7 without the proposed modification.

Introducing the proposed modification, which defines “activity” as “any activity offered by a website or online service, whether that activity is a subset or component of the website or online service or is the entirety of the website or online service,” may inadvertently introduce complexities and challenges, especially as technology continues to evolve.

As an example, consider emerging technologies beyond traditional websites and online services, such as virtual reality experiences,³⁷ augmented reality applications,³⁸ or other innovative platforms that may not neatly fit into the current understanding of a website or online service. Defining “activity” with such specificity could potentially limit the scope and applicability of the Rule in the future.

We recommend maintaining flexibility by not narrowing the definition further. By leaving the term “activity” open-ended, the Rule can adapt to new and evolving technologies on a case-by-case basis. This approach allows for a more dynamic and responsive regulatory framework, ensuring that the Rule remains effective in addressing emerging challenges without the need for frequent updates.

In summary, we suggest retaining the current definition of “activity” without the proposed modification to allow for flexibility and adaptability as technology evolves. This approach will enable a more pragmatic and case-specific assessment of activities offered by websites or online services.

³⁷ Virtual Reality in Education, Class VR, <https://www.classvr.com/virtual-reality-in-education/> (last visited Feb. 20, 2024); Virtual Reality in Education: Benefits, Tools and Resources, American University (Dec. 16, 2019), <https://soeonline.american.edu/blog/benefits-of-virtual-reality-in-education/>.

³⁸ Augmented Reality in Education, Maryville University (Mar. 12, 2021), <https://online.maryville.edu/blog/augmented-reality-in-education/>.

D. Conclusion

We thank the Commission for the opportunity to provide comments on its implementation of COPPA through the COPPA Rule. We appreciate the consideration of our comments during the COPPA Rule review process and look forward to working collaboratively with the Commission to protect children.

Respectfully submitted,



Ellen F. Rosenblum
Oregon Attorney General



Jonathan Skrmetti
Tennessee Attorney General



Kwame Raoul
Illinois Attorney General



Lynn Fitch
Mississippi Attorney General



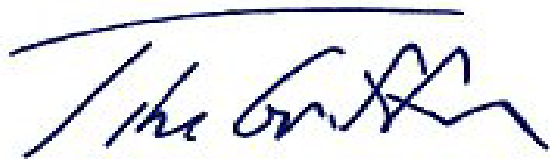
Steve Marshall
Alabama Attorney General



Treg R. Taylor
Alaska Attorney General



Kris Mayes
Arizona Attorney General



Tim Griffin
Arkansas Attorney General



Rob Bonta
California Attorney General



Phil Weiser
Colorado Attorney General



William Tong
Connecticut Attorney General



Kathleen Jennings
Delaware Attorney General



Brian Schwalb
District of Columbia Attorney General



Ashley Moody
Florida Attorney General



Christopher M. Carr
Georgia Attorney General



Anne E. Lopez
Hawaii Attorney General



Todd Rokita
Indiana Attorney General



Russell Coleman
Kentucky Attorney General



Aaron M. Frey
Maine Attorney General



Anthony G. Brown
Maryland Attorney General



Andrea Joy Campbell
Massachusetts Attorney General



Dana Nessel
Michigan Attorney General



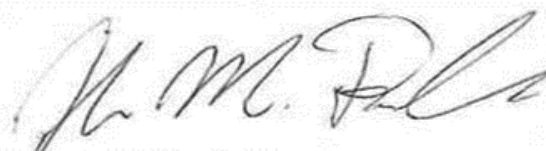
Keith Ellison
Minnesota Attorney General



Mike Hilgers
Nebraska Attorney General



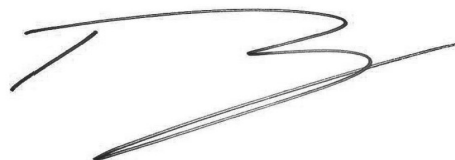
Aaron D. Ford
Nevada Attorney General



John M. Formella
New Hampshire Attorney General



Matthew J. Platkin
New Jersey Attorney General



Raúl Torrez
New Mexico Attorney General



Letitia James
New York Attorney General



Josh Stein
North Carolina Attorney General



Dave Yost
Ohio Attorney General



Gentner Drummond
Oklahoma Attorney General



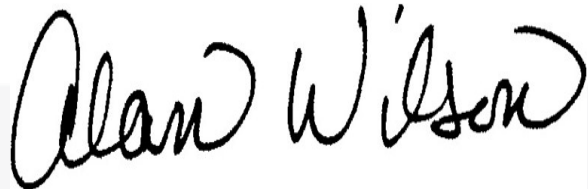
Michelle Henry
Pennsylvania Attorney General



Domingo Emanuelli-Hernández
Puerto Rico Attorney General



Peter F. Neronha
Rhode Island Attorney General



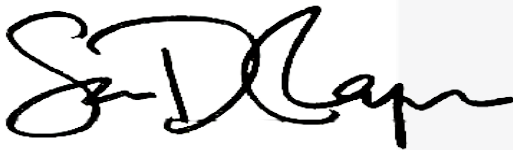
Alan Wilson
South Carolina Attorney General



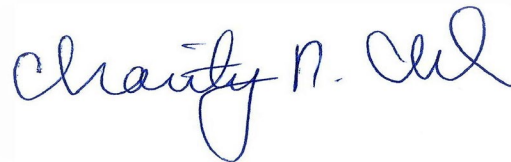
Marty Jackley
South Dakota Attorney General



Ariel M. Smith
U.S. Virgin Islands Attorney General



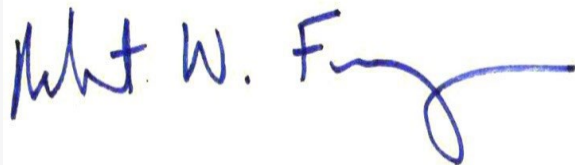
Sean D. Reyes
Utah Attorney General



Charity Clark
Vermont Attorney General



Jason S. Miyares
Virginia Attorney General



Robert W. Ferguson
Washington Attorney General



Joshua L. Kaul
Wisconsin Attorney General