



March 11, 2024

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

RE: COPPA Rule Review, Project No. P195404

The Interactive Advertising Bureau (IAB) welcomes this opportunity to submit this comment in response to the Federal Trade Commission’s request for public comment on its proposed changes to the Children’s Online Privacy Protection Rule (“NPRM”).¹ Founded in 1996 and headquartered in New York City, the IAB (www.iab.com) represents over 700 leading media companies, brand marketers, agencies, and technology companies that are responsible for selling, delivering, and optimizing digital advertising and marketing campaigns. Together, our members account for 86 percent of online advertising expenditures in the United States. Working with our member companies, the IAB develops both technical standards and best practices for our industry. In addition, the IAB fields critical consumer and market research on interactive advertising, while also educating brands, agencies, and the wider business community on the importance of digital marketing. The organization is committed to professional development and elevating the knowledge, skills, expertise, and diversity of the workforce across the digital advertising and marketing industry. Through the work of our public policy office in Washington, D.C., IAB advocates for our members and promotes the value of the interactive advertising industry to legislators and policymakers.

IAB shares the Commission’s commitment to protecting children online and looks forward to working with the FTC as it seeks to ensure the Rule continues to protect children as technologies advance. Online data-driven advertising has powered the growth of the Internet for decades by funding innovative tools and services for consumers to use to connect, learn and communicate, including websites and online services for children. Data-driven advertising supports and subsidizes the online content and services consumers, including children, rely on and expect. Regulation that impedes data-driven advertising has the potential to disrupt or decrease the varied and enriching content children can access and learn from online. We provide the following comments against this backdrop, highlighting important considerations for the Commission to take into account before finalizing the proposed changes to the Children’s Online Privacy Protection Rule.

¹ Trade Regulation Rule on the Use of Consumer Reviews and Testimonials, 88 Fed. Reg. 49364 (July 31, 2023) (hereinafter “NPRM”).”.

I. The FTC Rightly Concluded that “Actual Knowledge” is the Appropriate Standard for General Audience Services.

We appreciate the FTC re-affirming its longstanding view that “actual knowledge” is the appropriate standard required by the statutory text.² A constructive knowledge standard would be harmful to all consumers, including children. For example, a constructive knowledge standard would, counterintuitively, be more privacy invasive because it would incentivize companies to solicit more information than they otherwise might need, in an attempt to determine user age. A constructive knowledge standard would also incentivize companies to self-censor, in tension with fundamental First Amendment principles.³ Such self-censorship would diminish the accessibility of the Internet to children and young adults at a moment when teaching young people to safely navigate and harness the power of the Internet is more important than ever. Moreover, it would decrease the vibrancy and utility of the Internet for adult audiences as well, by chilling their online experience.

II. The FTC Should Further Clarify the Definition of “Personal Information” as it relates to Biometric Data, Screen and User Names, Avatars, and Inferred Data.

The FTC proposes several sweeping changes to the COPPA Rule’s “personal information” definition to address biometric data, screen and user names, avatars, and inferred data. As proposed, these changes are inconsistent with the text of the COPPA statute, FTC guidance, and related legislative changes currently being considered by Congress. The proposed changes also would have the apparently unintended effect of encouraging operators to collect more sensitive personal information, in tension with COPPA’s intended goal of promoting children’s privacy online. For these reasons, the proposed Rule should be further clarified, as detailed below.

A. The Biometric Identifier Addition Exceeds the FTC’s Statutory Authority, and Creates Inconsistencies with State Privacy Laws and FTC Guidance.

The NPRM’s insertion of “[a] biometric identifier that can be used for the automated or semi-automated recognition of an individual, including fingerprints or handprints; retina and iris patterns; genetic data, including a DNA sequence; or data derived from voice data, gait data, or facial data” into the definition of “personal information” exceeds the FTC’s statutory authority and creates inconsistencies with state privacy laws and FTC guidance.⁴ Rather than add an overly broad concept of biometric identifiers to the definition of “personal information,” the FTC should defer to the judgment of the U.S. Congress, which is actively considering the scope of biometric data covered under child protection laws, by declining to make such an addition in this proceeding.

² 89 Fed. Reg. 2034, 2037 (Jan. 11, 2024).

³ See, e.g., *New York Times Co. v. Sullivan*, 376 U.S. 254, 266, 279 (1964).

⁴ 89 Fed. Reg. 2034, 2041 (Jan. 11, 2024).

The proposed Rule would exceed the FTC’s statutory authority. The COPPA statute is explicit that the FTC only has the authority to add identifiers to the definition of personal information that “permit[] the physical or online contacting of a specific individual.”⁵ It is not enough under the statute that the identifier can be used to recognize an individual. Rather, the identifier must permit physical or online contacting of a specific individual. The FTC has not demonstrated this high standard is met with respect to the various elements included in the proposed biometric identifier definition. For example, while a text transcript derived from voice data (such as the text request “what day is President’s Day” derived from a voice input) is not a biometric identifier, the overly broad proposed language regarding data derived from voice data creates uncertainty. Such a broad interpretation would not meet the statutory standard of permitting the online or physical contacting of a specific person. As another example, the number of steps a child has taken derived from gait data does not permit online or physical contacting of that particular child (if indeed such information could be used to identify a child at all). Because such information does not satisfy the statutory standard, the FTC cannot include such information in the definition of “personal information.”

The NPRM purports to find support for this language in existing state privacy laws.⁶ However, such laws cannot expand the limited bounds of the Commission’s authority under COPPA, which rests in the text of the COPPA statute alone and requires that the identifier permit “the physical or online contacting of a specific individual.” It is the intent of Congress that must guide the Commission, and state laws have no bearing on the substance of a federal rulemaking. Moreover, the proposed biometric identifier addition would create adverse consequences. First, contrary to the NPRM’s suggestion, the proposed language in fact is broader than, and therefore creates potentially confusing inconsistencies with, existing state privacy laws.⁷ For instance, the proposed Rule is much broader than the Illinois Biometric Information Privacy Act (BIPA). BIPA explicitly excludes photographs, which the Rule includes.⁸ Moreover, BIPA defines a biometric identifier to include only the following data: “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.”⁹ Although BIPA also contains a definition for “biometric information” that captures certain derived information, it does so only where the information is derived from the specified biometric identifiers and only where such information on its own is used to identify an individual.¹⁰ The proposed Rule notably omits these important limitations and encompasses any information that can be used to recognize an individual, which significantly and impermissibly broadens the scope of the definition of personal information.

Moreover, state privacy laws and regulations such as those in Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, Virginia, and

⁵ 15 U.S.C. § 6501(8)(F).

⁶ 89 Fed. Reg. 2034, 2041 (Jan. 11, 2024).

⁷ These inconsistencies also create uncertainty regarding whether the proposed Rule would preempt state laws.

⁸ 740 ILCS 14/10.

⁹ 740 ILCS 14/10.

¹⁰ 740 ILCS 14/10.

Washington all exclude photos, videos, and audio recordings from their definitions.¹¹ Data derived from photos or recordings is considered biometric, if at all, only where it is used or intended to be used to identify a specific individual. For example, under Washington’s biometric privacy law, “biometric identifier” means data “generated by automatic measurements of an individual’s biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual.”¹² “Biometric identifier” does not include a physical or digital photograph, video or audio recording or data generated therefrom.¹³

Even California, whose definition of biometric information is arguably the broadest of all existing state laws, does not capture derived data and regulates gait patterns only where such data is used to “establish individual identity.”¹⁴ Thus, the FTC’s proposed definition creates inconsistencies with existing state privacy laws by including information derived from voice, gait, and facial data, even where such data does not, on its own, permit the identification of a specific individual, much less the physical or online contacting of that individual.

The proposed definition is also at odds with other aspects of the NPRM. For example, the FTC rightly concluded that inferred data and data that is a proxy for personal information cannot itself be “personal information” under COPPA, yet nevertheless proposes to treat such data as “biometric identifier” personal information to the extent it is derived from voice data, gait data, or facial data. The proposal is also inconsistent with the FTC’s 2017 Enforcement Policy Statement Regarding the Applicability of the Rule to the Collection and Use of Voice Recordings, which the FTC proposes to incorporate into the updated COPPA Rule. The Enforcement Policy Statement provides that, even though the FTC added audio files containing a child’s voice to the definition of “personal information” in the 2013 revisions to the COPPA Rule, the FTC will not require parental notice and consent to collect voice recordings from a child as a replacement for text inputs, as long as the voice recordings are deleted promptly after responding to the child’s request.¹⁵ The NPRM proposes to codify this Policy Statement and expand it to cover voice recordings even when they are not used as a substitute for written words. Treating all information derived from voice data as “biometric” personal information, regardless of whether it is used to identify or contact a specific person, is at odds with the FTC’s intent to permit the collection and processing of voice

¹¹ 4 CCR 904-3 Rule 2.02; Conn. Gen. Stat. § 42-515(3); Del. Code 6 § 12D-102(3); Fla. Stat. § 501.702(4); Ind. Code Ann. § 24-15-2-4(b); Iowa Code Ann. § 715D.1(4); Mont. Code Ann. § 30-14-2801(2)(3)(b); OR SB 619 § 1(3)(b); Tenn. Code Ann. § 47-18-3201(3)(B); Tex. Bus. & Com. Code § 541.001.3; Utah Code Ann. § 13-61-101(6)(c); Va. Code Ann. § 59.1-575; RCW § 19.375.010(1).

¹² RCW 19.375.010.

¹³ RCW 19.375.010.

¹⁴ Cal. Civ. Code § 1798.140(c).

¹⁵ *Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings*, 82 Fed. Reg. 58076 (Dec. 8, 2017), available at https://www.ftc.gov/system/files/documents/public_statements/1266473/coppa_policy_statement_audiorecordings.pdf.

recordings and to encourage the use of innovative, more accessible alternatives to text-based inputs.

The proposed definition also is inconsistent with a pending amendment to the COPPA statute that Congress is currently considering. If enacted, the proposed legislation would amend the “personal information” definition to include “[i]nformation generated from the measurement or technological processing of an individual’s biological, physical, or physiological characteristics that is used to identify an individual, including— (I) fingerprints; (II) voice prints; (III) iris or retina imagery scans; (IV) facial templates; (V) deoxyribonucleic acid (DNA) information; or (VI) gait.”¹⁶ This language significantly does not use the word “biometric” at all, and would require that the specified information be used to identify the child. The FTC should avoid making changes to COPPA that could end up diverging from the express intent of Congress. Because the bill text has not yet been enacted but is under active consideration, we urge the FTC to refrain from adding biometric identifiers to the definition of “personal information” at this time and instead defer to Congress on whether COPPA’s definition should be expanded.

B. Screen Names and User Names Should Not Be Treated as Personal Information Unless the Operator Uses Them as Online Contact Information.

The NPRM seeks comment on whether the definition of personal information should be modified to include screen or user names. The stated rationale for this change is that users and other third parties potentially could use screen or user names as online contact information, even if the particular operator collecting the information does not use the information for such purposes.¹⁷ As explained below, this extremely broad interpretation would fundamentally change how services operate on the Internet, resulting in a reduction of children’s privacy (contrary to the intent of COPPA), a dramatic increase in the number of services that will need to obtain verifiable parental consent, and a nullification of the support for internal operations exception.

There is no reasonable way for an operator to determine whether a particular child has used the same screen or user name across different sites or services. Even if the operator were hypothetically able to search and find the same screen or user name on a different service, there is no way for an operator who has not collected any additional personal information to verify whether it is the same user across these different services. Moreover, an interpretation that would not treat a screen or user name as personal information the first time an individual uses it, but that converts it to personal information the second time they do so, would create an unworkable and impractical regulatory regime. As a result, the practical effect of the proposed change would seemingly be to treat all screen and user names as “personal information” requiring verifiable parental consent.

Such a result would directly frustrate COPPA’s data minimization goals. Many operators collect an anonymous username or screen name precisely to avoid collecting personal information—such as a full name or email address—when such information is not otherwise needed for the child to engage in the particular activity. Yet, under this proposed change, operators would need to collect more personal information from the child and their parent than otherwise

¹⁶ Children and Teens’ Online Privacy Protection Act, S. Res. 1418, 118th Cong. (2023).

¹⁷ 89 Fed. Reg. 2034, 2070 (Jan. 11, 2024).

would be collected in order to seek verifiable parental consent, since an anonymous username or screen name is not sufficient to enable the operator to contact a parent to request verifiable parental consent.

Moreover, many operators that rely on the support for internal operations exception enable children to sign up with an anonymous screen or user name and otherwise collect only persistent identifiers to (for example) maintain and analyze the child's use of the service and manage the child's account preferences and similar personalized settings. If screen and user names are treated as personal information even when an operator does not use such information to contact a child, it would seem to nullify that operator's ability to rely on the support for internal operations exception. To avoid needing to collect additional personal information or verifiable parental consent, operators may instead choose to not offer their services to children at all, effectively rendering broad swaths of the Internet inaccessible to children. Such a result would undermine First Amendment principles and be contrary to Congress's intent that COPPA protect children's privacy online "in a manner that preserves the interactivity of children's experience on the Internet and preserves children's access to information in this rich and valuable medium."¹⁸

As recently as 2013, the FTC defended operators' ability to use anonymous screen and user names. In its COPPA rulemaking that year, the FTC updated the definition of personal information to include "screen or user name where it functions in the same manner as online contact information." At the time, commentators expressed concern that the update would preclude the use of anonymous screen names or the use of screen or user names to enable moderated or filtered chat and multiplayer game modes.¹⁹ In response, the Commission clarified that the Rule's current language "permits operators to use anonymous screen and user names in place of individually identifiable information, including use for content personalization, filtered chat, for public display on a Web site or online service, or for operator-to-user communication via the screen or user name."²⁰

However, by treating screen or user names as "personal information" even where that information does not permit contacting on the operator's website or online service, the current proposal would sweep in those very same anonymous screen and user names, preventing operators from undertaking the important functions that the Commission wished to protect in 2013. Instead, operators would be forced to regard all screen and user names as personal information under COPPA, and, counterintuitively, to seek verifiable parental consent for functions expressly designed to maintain children's safety and anonymity online. Accordingly, the definition of personal information should not be modified to include screen or user names that do not permit contacting by users and other third parties on the operator's website or online service.

C. Avatars Generated from a Child's Image Should Not Be Treated as Personal Information.

¹⁸ 144 Cong. Rec. S12787 (daily ed. Oct. 21, 1998) (statement of Sen. Bryan).

¹⁹ 78 Fed. Reg. 3972, 3979 (Jan. 17, 2013).

²⁰ 78 Fed. Reg. 3972, 3979 (Jan. 17, 2013).

The NPRM seeks comment on whether an avatar generated from a child’s image should constitute “personal information” even if the photograph of the child is not itself uploaded to the site or service and no other personal information is collected from the child.²¹ As explained further below, avatars do not constitute “individually identifiable information about an individual,”²² as the statutory definition of “personal information” requires. Additionally, if the image of the child in question does not leave the device, no personal information is “collected” under COPPA. Furthermore, allowing users to create avatars generated from an image is a privacy-protective alternative that should be encouraged, consistent with data minimization principles and FTC guidance encouraging blurring or other modifications to a child’s image before it is publicly displayed. For these reasons, the FTC should not adopt this proposal.

The FTC lacks a statutory basis for including avatars in the Rule’s definition of personal information. As discussed, the statute permits the FTC to expand the definition of “personal information” only where the information, on its own, is “individually identifiable” and “permits the physical or online contacting of a specific individual.”²³ There is no demonstration that an avatar generated from an image satisfies either requirement. To the contrary, operators utilize such avatars, similar to anonymous user and screen names, to allow a user to personalize their settings and experiences (such as game leaderboards and filtered or moderated chat) without collecting identifiable information.

An avatar is notably distinct from other types of information that the FTC has previously added to the Rule’s “personal information” definition. Whereas photographs were added to the definition of personal information in 2013 on the basis that a photo could “be paired with facial recognition technology” to “permit the physical or online contacting of a specific individual,”²⁴ an avatar, even when paired with facial recognition technology, cannot permit physical or online contacting of a specific individual. The features of a digital avatar are significantly abstracted from, and therefore cannot be associated with, those of the child represented by the avatar.

The NPRM attempts to overcome this statutory deficiency by emphasizing such avatars are derived from photos containing a child’s image. But photos are not “personal information” under the COPPA statute; they were added by regulation in 2013. And the reasoning is deficient regardless for at least three reasons. First, processing personal information (including photographs containing a child’s image) locally (i.e., on the user’s device) cannot trigger COPPA because the statute requires that personal information must be collected, used, or disclosed on the “Internet.”²⁵ The proposed expansion of the COPPA Rule to cover photographs that do not leave the device

²¹ 89 Fed. Reg. 2034, 2070 (Jan. 11, 2024).

²² 16 C.F.R. § 312.2.

²³ 15 U.S.C. § 6501(8).

²⁴ 78 Fed. Reg. 3972, 3981 (Jan. 17, 2013).

²⁵ See 15 U.S.C. § 6501(6) (defining “Internet”); Fed. Trade Comm’n, *Complying with COPPA: Frequently Asked Questions* F.5, <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>.

(and are therefore processed only locally) directly contradicts the FTC’s longstanding guidance and COPPA’s statutory limits.

Second, the FTC has recognized that, even if an operator collects a child’s image online, the operator can avoid triggering COPPA as long as the operator deletes the image before it is publicly displayed. For example, when the Commission added photos containing a child’s image to the COPPA Rule in 2013, it also explained that an operator “does not need to notify parents or obtain their consent if it blurs the facial features of children in photos before posting them on its website.”²⁶ Similarly, the FTC has long held that an operator may use reasonable filtering tools to otherwise remove personal information from a child’s post without triggering COPPA. This approach appropriately encourages operators to use data minimization techniques to enable highly valuable and interactive online experiences for children, while also protecting their privacy. Avatar creation is offered as an alternative to displaying an image of the child, and should thus be encouraged.

Third, treating an avatar derived from an image of a child is inconsistent with the FTC’s conclusion in the NPRM that a proxy for personal information cannot itself be “personal information” under COPPA.²⁷ While the photo provided by the child might be “from” the child within the meaning of the COPPA statute, the avatar that is derived therefrom is not. Accordingly, it cannot be restricted under COPPA. For these reasons, an avatar generated from a photo should not be treated as personal information.

D. The FTC Should Clarify That Its Approach to Inferred Data and Proxy Data Will Not Interfere with COPPA’s Support for Internal Operations Exception.

The FTC correctly concluded in the NPRM that inferred data and data that is a proxy for personal information cannot itself be “personal information” under COPPA.²⁸ As the Commission recognized, expanding the definition of “personal information” to include this information would go beyond the statutory text requiring that personal information be collected “from” a child.²⁹

Nevertheless, the Commission also stated in the NPRM that “[i]nferred data or data that may serve as a proxy for ‘personal information’ could fall within COPPA’s scope . . . if it is combined with additional data that would meet the Rule’s current definition of ‘personal information.’ In such a case, the existing ‘catch-all’ provision of that definition would apply.”³⁰

²⁶ 78 Fed. Reg. 3972, 3982 n.123 (Jan. 17, 2013) (“The Commission believes that operators who choose to blur photographic images of children prior to posting such images would not be in violation of the Rule”); *see also* Fed. Trade Comm’n, *Complying with COPPA: Frequently Asked Questions* F.3, <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>.

²⁷ 89 Fed. Reg. 2034, 2042 (Jan. 11, 2024).

²⁸ 89 Fed. Reg. 2034, 2042 (Jan. 11, 2024).

²⁹ 89 Fed. Reg. 2034, 2042 (Jan. 11, 2024).

³⁰ 89 Fed. Reg. 2034, 2042 (Jan. 11, 2024).

This statement not only mischaracterizes the statute’s catch-all provision, but also would appear to inadvertently nullify COPPA’s support for internal operations exception.

The COPPA statute defines “personal information” to include information combined with other identifiers described in the definition only if that information (1) is concerning the child or the parents of that child and (2) is information “that the website collects online from the child.”³¹ Thus, even if inferred or proxy data is combined with other enumerated identifiers, it would still not fall within COPPA’s “catch-all” provision. As the FTC acknowledges, “to the extent data is collected from a source other than the child, such information is outside the scope of the COPPA statute and such an expansion would exceed the Commission’s authority.”³² A definition of “personal information” broadened to include such information would dramatically diverge from the FTC’s existing concept of “personal information.”

Moreover, treating inferred and proxy data as “personal information” under COPPA’s catch-all would inadvertently eviscerate COPPA’s support for internal operations exception. We appreciate the FTC re-affirming that fraud prevention, product improvement, ad attribution, payment and delivery functions, optimization, and statistical reporting are all covered by the existing support for internal operations definition. These activities are necessary to achieve the FTC’s goal of ensuring “the smooth functioning of the Internet, the quality of . . . [a] site or service, and the individual user’s experience.”³³ However, each of these activities requires the combination of persistent identifiers with other inferred or proxy data. For example, fraud prevention may require the combination of an IP address with inferred data about whether the user’s behavior on the website is malicious. If such data were to be considered “personal information,” important safety-promoting activity currently protected by the support for internal operations exemption would be at risk. Operators of all kinds may refrain from engaging in fraud protection activities that protect consumers – including children – for fear of adverse enforcement actions. Accordingly, we request that the Commission clarify that the processing of inferred data and information that serves as a proxy for personal information does not fall within COPPA’s catch-all definition and does not undermine the support for internal operations exception.

III. User Reviews and Age Demographics of Other Services are not Competent and Reliable Indicators of Child-Directedness.

The Commission rightly concluded that use of a multi-factor test, under which no single factor is determinative, remains the appropriate standard for determining whether a service is child-directed.³⁴ The Commission should not, however, afford weight under the multi-factor test to reviews by users or third parties or to the age of users on similar websites or services. Neither are reliable or representative indicators of a service’s actual audience, and placing emphasis on either criterion would lead to arbitrary and capricious results.

³¹ 16 CFR § 312.2 (emphasis added).

³² 89 Fed. Reg. 2034, 2042 (Jan. 11, 2024).

³³ 78 Fed. Reg. 3972, 3980 (Jan. 17, 2013).

³⁴ 89 Fed. Reg. 2034, 2046 (Jan. 11, 2024).

User reviews are not reliable or competent evidence of a service’s audience demographics for a variety of reasons. First, an individual review (or even multiple reviews) frequently are not representative of the entire user base for a service. For instance, a handful of user reviews, or even hundreds of reviews if a service has millions of users, indicating that a child might use the service is not compelling evidence of a service’s complete audience demographics.³⁵ It is unclear how many reviews would need to discuss use by children in order to result in a child-directed finding, creating further ambiguity. It also is unclear how the FTC would determine which reviews to consider when evaluating a given service’s status, as there could be hundreds or thousands of individual reviews from which to choose, each of which might lead to different conclusions about the nature of the site or service. Relying on a small or cherry-picked set of user reviews imposes an impossibly high degree of ambiguity and arbitrariness on operators attempting to assess their COPPA compliance. In addition, it’s unclear how the FTC would deal with the practice of review bombing, in which fake accounts leave large quantities of negative or false reviews, which could be used to force a company into COPPA compliance even if, in fact, its audience is not mainly composed of children.³⁶ Indeed, the FTC observed in another recent proceeding that “fake consumer reviews and testimonials, as well as reviews and testimonials that otherwise misrepresent the experiences of the reviewers and testimonialists, are prevalent.”³⁷

Second, relying on user reviews will introduce ambiguity and uninformed subjective opinion into the child-directedness test. Users are not familiar with the legal nuances of COPPA, but may write reviews that have unintended legal implications. For example, if a parent allows their child to use the child-directed portion of an otherwise general audience service, they may leave a review saying “my child enjoyed this service” without explaining that their child only accessed the child-directed portion. Or the parent of a teenager might write a user review saying “my child loves this game” not realizing that “child” is a term of art under COPPA. A user review expresses, at best, the user’s subjective views and experience, which is not competent evidence of the actual audience demographics of the entire website or online service.

Third, relying on user reviews inadvertently and improperly introduces a constructive knowledge standard into the COPPA Rule. As the FTC has repeatedly recognized, including most recently in the NPRM itself, the COPPA statute plainly requires “actual knowledge” for general audience sites and services.³⁸ The FTC also has repeatedly acknowledged that a service is not child-directed simply because some children use the service and that operators of general audience

³⁵ Fed. Trade Comm’n, *Complying with COPPA: Frequently Asked Questions* D.3, <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#C.%20Privacy%20Policies> (“Your website or online service will not be considered “directed to children” just because some children visit your site or use your service”).

³⁶ Jim Zarroli, Goodreads has a ‘review bombing problem – and wants its users to help solve it, NPR: All Things Considered (Dec. 17, 2023), <https://www.npr.org/2023/12/17/1219599404/goodreads-review-bombing-cait-corrain>.

³⁷ 88 Fed. Reg. 49364, 49373 (Jul. 31, 2023).

³⁸ 89 Fed. Reg. 2034, 2037 (Jan. 11, 2024).

services have no duty to investigate the ages of their users.³⁹ Yet, the proposed modification to the COPPA Rule would contradict each of these longstanding principles. Services are often unaware of the contents of each user review. But the NPRM seems to imply that operators have a duty to investigate user reviews in order to assess whether they are child directed; that customer reviews may provide an operator reason to know it collects personal information from children; and that this constructive knowledge should trigger COPPA obligations for such operators by treating them as child-directed instead of directed to a general audience. Imposing requirements on services that have a “reason to know they may be collecting information from a child” is exactly how the NPRM defines constructive knowledge,⁴⁰ a standard that the FTC has explicitly and repeatedly rejected. It is illogical for the FTC to denounce the constructive knowledge standard while simultaneously introducing it into the child-directed criteria instead.

For all of these reasons, the Commission should not afford any weight to user reviews when assessing whether a service is child-directed.

The audience composition of other sites and services also has no reliable bearing on whether a particular service is child-directed. And the standard in the proposed Rule is vague and could lead to arbitrary results. First, a company cannot access competitors’ internal audience composition data and thus has no way of knowing the audience composition of similar sites and services. Moreover, external indicators such as user reviews are not even a reliable way of determining a company’s own audience composition, let alone that of a competitor, as discussed above. External surveys or reports are also often unreliable, biased, and unrepresentative. Thus, companies lack a reliable method of establishing actual knowledge of the audience composition of other sites or services – at a moment of time, let alone on an ongoing basis – meaning that this factor would, in practice, impose a constructive knowledge standard. Second, the NPRM does not specify what would make one service sufficiently “similar” to another, and there is no principled method for determining when two services are sufficiently similar such that the demographic data for one service should be attributed to another. For example, two websites could each offer an online crossword puzzle. Even though the services are “similar” because they offer the same activity, other facts and circumstances might result in material differences in their user demographics. For example, if one operator markets its crossword puzzle site for use in elementary school classrooms, using child celebrities, or using promotional materials in other child-directed media, it might have a very large number or percentage of child users. In contrast, if the other operator markets its crossword puzzle site to retirees, the audience demographics are likely to be much different. Third, it is not clear whether or how the FTC’s analysis could fully capture the varied and numerous reasons why one service’s age demographics might be different from another’s. Furthermore, any factors that could be relied upon in such an analysis, such as examination of marketing strategies, are already reflected in the other criteria included in the multi-factor test, creating unnecessary redundancy and complexity. Because analysis of similar services would be inherently unreliable and arbitrary, it should not be considered in the FTC’s analysis.

³⁹ Fed. Trade Comm’n, *Complying with COPPA: Frequently Asked Questions* D.3 and E.2, <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#C.%20Privacy%20Policies>.

⁴⁰ 89 Fed. Reg. 2034, 2037 (Jan. 11, 2024).

The problematic nature of these changes becomes clear when they are evaluated together. If the FTC considers the age of users on similar sites or services in assessing child-directedness, and the child-directedness of those similar sites is determined by their own user reviews, that would suggest that a company must examine the user reviews of similar sites and services to determine its own child-directedness. Requiring a company to evaluate child-directedness based on reviews of its own sites and services already introduces unreliability and imposes a constructive knowledge standard, as explained above. Requiring companies to first determine all similar sites and services and then scour the Internet for user reviews of those similar sites and services to determine if its own sites and services may be child-directed effectively renders it impossible for companies to assess their status under the child-directedness test.

IV. The “Mixed Audience” Definition Must Incorporate Prior FTC Guidance to Avoid Expanding the Rule Beyond Statutory and Constitutional Limits.

The NPRM’s “mixed audience” definition appears intended to codify the FTC’s interpretation of its rules pertaining to mixed audience sites and services in the 2013 COPPA Rule proceeding.⁴¹ As drafted, however, the proposed definition loses important nuance regarding how a service will be found to be mixed audience. Specifically, in response to concerns raised in the public comments to the proposal for the 2013 COPPA Rule that the mixed audience designation would inappropriately expand the Rule beyond the statutory text and raise constitutional concerns, the FTC stated that “[t]he Commission did not intend to expand the reach of the Rule to additional sites and services, but rather to create a new compliance option for **a subset of Web sites and online services already considered directed to children under the Rule’s totality of the circumstances standard.**”⁴² To clarify this intention, the FTC enumerated a two-step process by which it will first apply its totality of the circumstances standard to determine whether the site or service is directed to children or to a general audience. If, and only if, the service is directed to children at that first step, will the FTC continue to the second step of applying the same totality of the circumstances criteria to assess whether children are the primary audience or whether the service is part of the subset of services directed to children as a secondary audience.⁴³

The proposed “mixed audience” definition does not clearly incorporate this two-step analysis. Without this clarification, it is unclear how the FTC will determine whether a child-directed service targets children as its primary or secondary audience, and the definition inadvertently could expand the reach of the COPPA Rule beyond the limits of what the COPPA statute and Constitution can bear. The Commission also should update the language to clarify that mixed audience sites and online services can continue to rely on the exceptions to prior parental consent contained in Section 312.5(c) of the COPPA Rule. Accordingly, the Commission should clarify the definition as follows and re-iterate its intention to not expand the reach of the COPPA Rule beyond the subset of sites and online services that are already considered child-directed:

“Mixed audience website or online service means a website or online service that, **only after applying** the criteria set forth in paragraph (1) of the definition of

⁴¹ 89 Fed. Reg. 2034, 2048 (Jan. 11, 2024).

⁴² 78 Fed. Reg. 3972, 3984 (Jan. 17, 2013) (bold emphasis added).

⁴³ 78 Fed. Reg. 3972, 3984 n.162 (Jan. 17, 2013).

website or online service directed to children **and determining such website or online service is directed to children, also targets children as a secondary audience for the site or service applying the same criteria. Mixed audience websites and online services shall** not collect personal information from any visitor prior to collecting age information or using another means that is reasonably calculated, in light of available technology, to determine whether the visitor is a child, **unless such collection is permitted under Section 312.5(c).** Any **collection of age information, or other** means of determining whether a visitor is a child, must be done in a neutral manner that does not default to a set age **at or above 13 years old** or encourage visitors to falsify age information.”

V. Age Estimation Standards are Privacy-Invasive, Unconstitutional, Unreliable, Biased, and Impractical.

While the Commission’s efforts to encourage (rather than require) companies to engage in age estimation⁴⁴ appear well-intended, we are concerned that any age assurance standards the FTC might endorse — even if voluntary — could inadvertently undermine the privacy of consumers, deter Internet usage, chill access to constitutionally protected speech, and perpetuate bias. Moreover, the implementation of a threshold-based exemption would be inconsistent with the FTC’s decision in the NPRM to retain COPPA’s multi-factor test, under which no single factor is determinative. The proposed exemption would consider only a single factor — namely audience demographics — resulting in this single factor being determinative. Such a result would be contrary to Congressional intent. Congress chose to define websites and online services “directed to children” narrowly by considering whether they are “targeted” to children, rather than premising the law’s coverage on user demographics, and the Commission must ensure consistency with this legislative intent.⁴⁵

First, age estimation techniques and age analysis is likely to result in an operator collecting more personal information than necessary for the requested activity, in tension with COPPA’s data minimization requirements. For example, a provider of an online game collecting only persistent identifiers may feel pressure to start collecting additional information to verify or assess the user’s age solely to benefit from the proposed exception, if enacted. The Commission should avoid encouraging operators to collect more information than they otherwise would need.

Second, incentivizing companies to collect additional information to assess age could chill access to constitutionally protected speech, as recognized by researchers and courts. Research has shown that even a short time delay in a user’s access to web content, such as the delay that would be caused by having a user provide additional age information, can drive users away and hinder their access to protected speech.⁴⁶ Moreover, some privacy-conscious individuals or individuals who lack certain forms of identification might not want to or be able to provide additional age

⁴⁴ 89 Fed. Reg. 2034, 2070 (Jan. 11, 2024).

⁴⁵ 15 U.S.C. § 6501(10).

⁴⁶ *See Will Co. v. Lee*, 47 F.4th 917, 924-25 (9th Cir. 2022) (“Research shows that sites lose up to 10% of potential visitors for every additional second a site takes to load, and that 53% of visitors will simply navigate away from a page that takes longer than three seconds to load.”).

verification information, potentially preventing them from accessing the full scope of services available on the Internet. Congress’s interest in preserving a vibrant Internet is thus at odds with age estimation.

Significantly, courts that have considered age estimation — whether as a requirement or as an incentive — have uniformly found such requirements to be unconstitutional restrictions on accessing speech. For example, the Northern District of California ruled, in considering the age estimation provisions of the California Age Appropriate Design Code Act (which strongly incentivized, but did not outright require, age estimation), that “the steps a business would need to take to sufficiently estimate the age of child users would likely prevent both children and adults from accessing certain content.”⁴⁷ Similarly, the Western District of Arkansas found that Arkansas’ age verification law “is likely to unduly burden adult and minor access to constitutionally protected speech.”⁴⁸ The Western District of Texas also struck down a Texas law requiring age verification to access pornographic content, stating that the result of the law “as applied to online webpages is that constitutionally protected speech will be chilled.”⁴⁹ Lastly, the Middle District of Louisiana enjoined a similar age verification law on the basis that it had “potential to lead to self-censorship” and that its vagueness would cast a “chill on protected speech.”⁵⁰

Third, the Commission should avoid encouraging age analysis techniques that could be unreliable. Experts agree that “there is currently no solution that satisfactorily” provides “sufficiently reliable verification, complete coverage of the population and respect for the protection of individuals’ data and privacy and their security.”⁵¹ Every contemplated method of age estimation is flawed. In fact, the Commission itself has recognized that self-reporting allows users to misreport their ages; document review excludes those without the requisite documentation; and automated estimation can be inaccurate and biased. For example, research on AI age estimation technology has found that AI estimated the ages of smiling faces as older than the neutral faces of the same people.⁵² Even international governments agree that the “market for age assurance products is immature.” The Australian government has stated that “at present, each

⁴⁷ *NetChoice, LLC v. Griffin*, No. 5:23-CV-05105, 2023 WL 5660155 at *21 (W.D. Ark. Aug. 31, 2023).

⁴⁸ *NetChoice, LLC v. Griffin*, No. 5:23-CV-05105, 2023 WL 5660155 at *21 (W.D. Ark. Aug. 31, 2023).

⁴⁹ *Free Speech Coal., Inc. v. Colmenero*, No. 1:23-CV-917-DAE, 2023 WL 5655712 at *11 (W.D. Tex. Aug. 31, 2023).

⁵⁰ *Garden Dist. Book Shop, Inc. v. Stewart*, 184 F. Supp. 3d 331, 338, 341 (M.D. La. 2016). See also *NetChoice, LLC v. Yost*, No. 2:24-CV-00047, 2024 WL 555904 (S.D. Ohio Feb. 12, 2024) (finding that certain parental consent requirements violated the First Amendment).

⁵¹ Jackie Snow, *Why Age Verification Is So Difficult for Websites*, Wall St. J. (Feb. 27, 2022), <http://bit.ly/41ngt5m>.

⁵² Tzvi Ganel, et al., *Biases in human perception of facial age are present and more exaggerated in current AI technology*, 12 Sci. Reps. 22519, 2022, [https://www.nature.com/articles/s41598-022-27009-w#:~:text=\(c\)%20Age%20estimation%20bias%20for,in%20AI%20compared%20to%20humans.](https://www.nature.com/articles/s41598-022-27009-w#:~:text=(c)%20Age%20estimation%20bias%20for,in%20AI%20compared%20to%20humans.)

type of age verification or age assurance technology comes with its own privacy, security, effectiveness and implementation issues,” and that such technology cannot, at this time, work reliably and balance privacy and security concerns.⁵³

Fourth, automated estimation systems can perpetuate bias, whether they rely on (for example) analysis of photos or user behavior. Research has found that when AI is used to determine age based on photos, the average AI performance sharply decreased for faces of older adults compared to faces of young and middle-aged adults.⁵⁴ A growing body of research has also demonstrated that face recognition algorithms are less accurate in subjects who are female or Black.⁵⁵ If companies avoid automated age estimation that relies on photos and instead focus on user behavior, additional issues arise. Attempting to determine age through inferences based on user’s behavior on the operator’s site or service could introduce its own biases as well as chill use of the platform.

Fifth, an exemption based on an operator’s age estimation analysis would be unduly burdensome. Small and medium-sized businesses that lack the resources to conduct sophisticated age analysis would find it especially difficult to take advantage of the exemption. If combined with the proposal to assess operators’ child-directedness by considering the audience composition of similar sites or services, the exemption imposes an even larger burden on small and medium sized operators. If large companies with the resources to conduct age estimation find their audience to consist heavily of children, small or medium sized businesses that provide similar services would be presumed child-directed, and would not have the resources to conduct the age estimation necessary to rebut that presumption. Furthermore, the implicit requirements for an operator to implement, maintain, and continuously audit their age estimation techniques, while maintaining detailed documentation of each such step could contradict the Paperwork Reduction Act’s mandate to minimize the federal information collection burden.

Sixth, the proposed exemption would be ambiguous in its application. Without further clarification, operators seemingly must continuously perform age estimation and assess their audience composition in order to maintain exempt status. Given that interest in websites and services can shift rapidly along with changing audience demographics, some operators could face substantial uncertainty with respect to their COPPA status. This concern would be particularly

⁵³ Australian Government, Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *Government Response to the Roadmap for Age Verification*, (Aug. 2023), <https://www.infrastructure.gov.au/sites/default/files/documents/government-response-to-the-roadmap-for-age-verification-august2023.pdf>. See also CNIL, *Online Age Verification: Balancing Privacy and the Protection of Minors* (Sept. 22, 2022) (similar), <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>.

⁵⁴ Tzvi Ganel, et al., *Biases in human perception of facial age are present and more exaggerated in current AI technology*, 12 *Sci. Reps.* 22519 (2022), [https://www.nature.com/articles/s41598-022-27009-w#:~:text=\(c\)%20Age%20estimation%20bias%20for,in%20AI%20compared%20to%20humans.](https://www.nature.com/articles/s41598-022-27009-w#:~:text=(c)%20Age%20estimation%20bias%20for,in%20AI%20compared%20to%20humans.)

⁵⁵ Alex Najibi, *Racial Discrimination in Face Recognition Technology*, Harvard University (Oct. 24, 2020), <https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/>.

salient to operators of websites and services whose audience percentages are very close to the FTC’s threshold, meaning that small fluctuations in audience composition could bring them in and out of the exemption’s coverage. Thus, if the FTC does elect to implement a threshold-based exemption, it should make clear that once an operator has conducted an analysis of user demographics, it may rely on that analysis for a definite period of time (*e.g.*, one year) before having to refresh it, and should have a one-year period to come into compliance if audience demographics change. The FTC should also defer to operators’ reasonable analyses of user demographics. Otherwise, operators would be subject to substantial uncertainty with respect to their compliance obligations and any exemption would become, in practicality, moot.

Moreover, while the FTC proposes that age analysis be a voluntary exercise, it would in practice likely become involuntary given the FTC’s proposal to consider the age demographics of “similar” services as part of the child-directedness test. If a competitor voluntarily chooses to conduct age analysis and such evaluation concludes that the competing service does not meet the threshold to be treated as an exempt general audience service, then the operator likely will feel pressured to conduct its own analysis to avoid having the competitor’s analysis attributed to it, even if the operator has taken steps to differentiate its audience composition from that of its competitor. The Commission should clarify that a company that does not choose to estimate age for the reasons detailed above will not face any additional scrutiny, presumption of child-directedness, or other prejudice. Otherwise, what is intended to be an optional exemption quickly would become mandatory in practice, despite the many costs it would impose on businesses.

VI. The NPRM’s Proposed Limitations on the Support for Internal Operations Exception Should be Narrowed or Eliminated.

The NPRM would impose significant new obligations on operators that make use of the support for internal operations exception to the Rule’s verifiable parental consent requirements. First, it would require operators to “specifically identify the practices for which the operator has collected a persistent identifier”⁵⁶ and describe how the operator ensures that the identifier is not used to contact a specific individual in a notice on the website or service. Second, the NPRM would prohibit operators from using the support for internal operations exception to “encourage or prompt use of a website or online service” by children or “optimize user attention or maximize user engagement” without parental consent.⁵⁷ Third, the NPRM seeks comment on whether the Commission should consider changes to the Rule’s treatment of contextual advertising, which is currently permitted under the Rule’s support for internal operations exception.⁵⁸

As explained in more detail below, each of these proposals should be further refined or reconsidered. The proposed disclosure requirements would undermine the security and stability of websites and services and create ambiguity in how COPPA will be enforced. Instead, operators should be able to satisfy the proposed disclosure requirements by identifying which of the enumerated activities in the “support for internal operations” definition they conduct. Furthermore, a broad prohibition on design choices that “encourage or prompt use” of a website

⁵⁶ 89 Fed. Reg. 2034, 2045 (Jan. 11, 2024).

⁵⁷ 89 Fed. Reg. 2034, 2045 (Jan. 11, 2024).

⁵⁸ 89 Fed. Reg. 2034, 2070 (Jan. 11, 2024).

or service would introduce an arbitrary and vague line-drawing exercise that would be operationally impractical and in tension with the statute and constitutional principles. And the Commission should not disturb the longstanding position that contextual advertising falls within the support for internal operations exception.

As the FTC has recognized repeatedly,⁵⁹ enabling operators to collect persistent identifiers to carry out the purposes laid out in the “support for internal operations” definition is “fundamental to the smooth functioning of the Internet, the quality of the site or service, and the individual’s user experience.” Thus, the FTC should clarify these proposals to avoid degrading the quality of services available on the Internet and threatening constitutionally protected activity.

A. The FTC Should Allow Operators to Satisfy the Disclosure Requirement by Referring to One or More of the Activities Included Under the Exception.

The FTC stated in the 2011 COPPA Rule NPRM that “the Commission does not intend to limit operators’ ability to collect” persistent identifiers “to aid the functionality and technical stability” of websites and services.⁶⁰ The support for internal operations exception was developed to cement that policy within the Rule. A broad interpretation of the contemplated requirements — particularly one that would require operators to provide a detailed description of “the practices for which the operator has collected a persistent identifier” — would undermine the purpose and usefulness of the exception.

Some of the most important activities covered by the support for internal operations exception are operators’ efforts to protect “the security and integrity of the user, website, or online service.”⁶¹ Read broadly, the new disclosure obligations proposed in the NPRM would frustrate this important use case by requiring operators to reveal previously nonpublic security practices. Bad actors may be able to leverage such disclosures to compromise websites and services or their users, particularly if the FTC requires that operators provide granular information about how they use persistent identifiers for security purposes. For example, an operator might rely on persistent identifiers to implement a system that detects suspicious login attempts or password changes. With sufficient knowledge of how the persistent identifiers are used, a bad actor may be able to tailor their attacks to circumvent the system.

Similarly, the 2013 revisions to the Rule stated that the support for internal operations exception permits operators to use persistent identifiers to “protect[] against fraud or theft”⁶² without first securing parental consent. The new disclosure requirements could make it easier for fraudsters to circumvent protections implemented by operators, including spam detection and transaction verification systems that enable operators to flag suspicious or exploitative activity before it causes harm.

⁵⁹ 78 Fed. Reg. 3972, 3980 (Jan. 17, 2013); 89 Fed. Reg. 2034, 2045 n.142 (quoting 78 Fed. Reg. at 3980).

⁶⁰ 76 Fed. Reg. 59804, 59809-10 (Sept. 27, 2011).

⁶¹ 16 C.F.R. § 312.12.

⁶² 78 Fed. Reg. 3972, 3979 (Jan. 17, 2013).

Other valuable uses of the exception involve identifying and resolving technical problems by “[m]aintain[ing] and analyz[ing] the functioning”⁶³ of a website or service. Given the fundamental unpredictability of debugging and other procedures associated with maintaining a website or service, operators need the flexibility to use persistent identifiers — including on a very short-term basis — to diagnose and investigate bugs and service interruptions. It would therefore be impossible for operators to specify in advance all of the granular ways in which they might use various persistent identifiers to ensure the stability of a website or service. If the FTC requires that operators provide such detailed information, it would risk severely undermining the quality and performance of websites and services by effectively prohibiting certain forms of debugging.

Moreover, ambiguity around the required level of specificity for disclosures made under the new requirements could create confusion in the enforcement context, potentially leading to unpredictable or arbitrary enforcement patterns that could burden access to lawful content. For example, the FTC has recognized that a variety of activities (such as fraud prevention, product improvement, ad attribution, payment and delivery functions, optimization, and statistical reporting) fall within the exemption permitting an operator to maintain and analyze the functioning of the site or service. It is unclear whether it is sufficient to specify that persistent identifiers are used to maintain and analyze service functionality, or whether an operator must elaborate further by specifying all the applicable activities in the enumerated examples or provide some other level of detail. Enforcement-related uncertainties could discourage operators’ use of the exception and deprive both children and their parents of its benefits, and potentially raise constitutional concerns by impairing their access to lawful content.

We are skeptical that any incremental benefits associated with more prescriptive, detailed disclosure requirements would outweigh these serious drawbacks. Adding new and potentially very technical information about the use of persistent identifiers to the already substantial disclosures required under COPPA would lengthen and complicate operators’ online notices, reducing rather than improving their usefulness to parents. Parents are unlikely to benefit from such technical information. The FTC should therefore clarify that operators can fully satisfy the disclosure requirements by specifying in which of the seven enumerated “support for internal operations” activities they engage. This approach would accomplish the NPRM’s objectives of “increas[ing] transparency” and “ensur[ing] that operators follow the use restriction”⁶⁴ without undermining the usefulness of the support for internal operations exception or adding ambiguity and arbitrariness to COPPA enforcement.

B. The FTC Should Either Eliminate the Prohibition on Using the Exception to “Encourage or Prompt” Use or Clarify that It Applies Only to Push Notifications.

The NPRM’s proposal to prohibit operators from relying on the support for internal operations exception to provide functions that “encourage or prompt use of a website or service” requires clarification. As drafted, the language of the prohibition is vague, and therefore does not give companies clear notice of which functions are prohibited. If applied broadly, the prohibition

⁶³ 16 C.F.R. § 312.12.

⁶⁴ 89 Fed. Reg. 2034, 2045 (Jan. 11, 2024).

could undermine user experiences across websites and services, exceed statutory limits, and be in tension with First Amendment principles. And because the NPRM also proposes to require that “to the extent an operator uses personal information collected from a child to encourage or prompt use of the operator’s website or online service . . . such use must be explicitly stated in the direct notice,”⁶⁵ as well as in the online notice,⁶⁶ this limitation to the exception would substantially limit the support for internal operations exception.

In its current form, the prohibition could be read expansively as applying to a wide range of design practices that benefit consumers, including “personalization” and “optimization” expressly permitted under the support for internal operations exception. Many useful user experience design choices could conceivably be understood to “encourage or prompt use of a website or service”: well-designed websites and services retain user interest by anticipating users’ preferences and needs. The NPRM suggests that the prohibition would extend to features that “optimize user attention,” an overbroad category that could be read as limiting features that seek to be engaging and entertaining to users (raising serious First Amendment questions), or even that simply seek to streamline and improve a user’s experience with a website or service. For example, platforms that host video content would be less useful to users if those platforms could not measure users’ previous views and avoid repeatedly offering up the same content.

Contributing to this potential overbreadth and ambiguity, the NPRM expressly states that at least some “machine learning processes” may fall within the scope of the prohibition, but does not define what those processes are.⁶⁷ If the prohibition is interpreted as limiting operators’ ability to use machine learning technologies to improve product offerings, it would negatively impact children’s experience using websites and services. For example, the use of machine learning processes to deliver closed captioning and other user accessibility features could be undermined under the proposed Rule. It could also impair operators’ ability to deploy features like personalized tutoring systems that adjust the content and difficulty of lessons to keep children appropriately challenged and engaged.

In addition to subjecting operators to ambiguous design limitations, a broad reading of the prohibition could go beyond COPPA’s intended scope and raise constitutional concerns. COPPA is intended to protect the privacy and safety of children’s personal information online, not to be a “design code” statute. An interpretation that would stretch the COPPA Rule into this uncharted territory would significantly overstep statutory authority and congressional intent. In essence, a broad reading of the prohibition would require the FTC to draw a line between those undefined design elements that the FTC deems user “friendly” and those undefined “engagement-enhancing techniques” that the FTC deems lead to “overuse” of services by children, a fraught task for which the statute provides no guidance whatsoever.⁶⁸ Application of the Rule in this domain is therefore

⁶⁵ 89 Fed. Reg. 2034, 2049 (Jan. 11, 2024).

⁶⁶ 89 Fed. Reg. 2034, 2050 (Jan. 11, 2024).

⁶⁷ 89 Fed. Reg. 2034, 2045 (Jan. 11, 2024).

⁶⁸ 89 Fed. Reg. 2034, 2059 n.300 (Jan. 11, 2024) (“The Commission is aware of recent media reports indicating that children may be overusing online services due to engagement-enhancing techniques. The Commission is concerned about the potential harm from such overuse and (continued...)”).

likely to produce vague, arbitrary, and capricious results. A broad interpretation also could unconstitutionally limit access to legal content online by making platforms that facilitate such access more difficult to use (*e.g.*, by limiting personalization).

Significantly, Congress is currently grappling with these very issues, not through COPPA, but by way of the Kids Online Safety Act (“KOSA”), the current draft of which imposes limitations on “features that result in compulsive usage of the covered platform by a minor.”⁶⁹ The FTC should defer to Congress and avoid implementing a prohibition that may clash with still-forming congressional prerogatives in this area.

If it chooses to retain this prohibition in the final Rule at all, we urge the FTC to specify that the prohibition is limited to push notifications that “encourage or prompt use of a website or online service” only. This approach would align with the examples provided in the NPRM and provide a clearer, more workable standard. However, we note that even this more limited approach could have adverse unintended consequences. For example, some educational apps use push notifications to keep children on track with their studies, including in conjunction with usage “streaks” and other systems intended to gamify learning for children’s benefit. Other apps prompt children to complete educational content before accessing entertainment content, which is intended to promote learning. Such apps may be found to encourage use of a service and thus not be able to rely on the support for internal operations, which seems to be an unintended consequence of the proposed Rule. Accordingly, the better approach is to defer to Congress on this issue.

C. The FTC Should Not Modify The Rule’s Treatment of Contextual Advertising Within The Support For Internal Operations Exception.

The NPRM requests comment on whether the FTC should “consider changes to the Rule’s treatment of contextual advertising” based on the proposition that “personal information collected from users may be used to enable companies to target even contextual advertising to some extent.”⁷⁰ As a threshold matter, the NPRM proposal does not provide sufficient notice of what a “change” to the support for internal operations exception for contextual advertising would entail, or what sorts of practices would constitute “targeting” of contextual advertisements.

The FTC has consistently recognized that the support for internal operations exception is “fundamental to the smooth functioning of the Internet, the quality of the site or service, and the individual’s user experience.”⁷¹ And we agree with the Commission’s conclusion in the NPRM that it “struck the proper balance in 2013 when it expanded the personal definition while also creating a new exception to the Rule’s requirements” for internal operations, including for contextual advertising. Maintaining this exception in its current form will incentive companies to

therefore deems it important to ensure parents are notified and provide verifiable parental consent before operators use such techniques to further children's engagement with websites and online services.”)

⁶⁹ Kids Online Safety Act, S. 1409 § 4(1)(C) (as reported to the Senate on Dec. 13, 2023).

⁷⁰ 89 Fed. Reg. 2034, 2070 (Jan. 11, 2024).

⁷¹ 78 Fed. Reg. 3998 (Jan. 17, 2013).

continue using a form of advertising that the FTC considers to be privacy protective as well as ensure the financial viability of providing high-quality, safe, age-appropriate content for children.⁷² Accordingly, the Commission should maintain its longstanding position that the use of a persistent identifier to deliver contextual advertisements falls within the support for internal operations exception.

VII. The NPRM’s New Data Retention Requirements may Raise Concerns Under the Paperwork Reduction Act and Should be Streamlined.

The NPRM proposes requiring that operators establish and maintain written data retention policies for children’s personal information. Such policies would need to indicate the business purposes for which personal information is retained and include a retention schedule. Operators would be required to provide the retention policy in their online notices. The NPRM also proposes to clarify that children’s personal information may only be retained for as long as is reasonably necessary for the business purpose for which it was collected, and that it may not be retained for any secondary purpose.⁷³

As a threshold matter, Congress is currently reexamining COPPA’s retention requirements as part of the current draft of the “COPPA 2.0” amendments.⁷⁴ The FTC should defer to Congress in addressing this issue and not engage in any further rulemaking on retention policies until Congress has been able to fully consider the pending legislation.

Should the FTC nonetheless decide to take up retention policies as part of this proceeding, it should bear in mind that the new written data retention policy requirement proposed in the NPRM would be burdensome to operators, raising concerns under the Paperwork Reduction Act. The NPRM substantially underestimates the compliance costs that such a requirement would impose on operators, stating that operators would need to invest on average approximately “10 hours to meet the data retention policy requirement.”⁷⁵ Drafting and maintaining a retention policy and retention schedules specific to children will likely take substantially longer, particularly where an operator uses data in several different ways across multiple services. The FTC should mitigate the burden to operators by clarifying that a general description of the purposes for which personal information is collected and a general statement of the operator’s retention timeframes suffices to satisfy the requirement. The FTC also should clarify that an existing data retention policy can

⁷² *Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009) (finding that contextual advertising, advertising based on a single search query, and first party advertising is “consistent with consumer expectations, and less likely to lead to consumer harm”), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>.

⁷³ 89 Fed. Reg. 2034, 2075 (Jan. 11, 2024).

⁷⁴ In some ways, the requirements proposed in the NPRM go beyond those contemplated by the “COPPA 2.0” amendments. For example, the most recent draft of COPPA 2.0 does not require that operators publish retention schedules. *See Children and Teens’ Online Privacy Protection Act*, S. 1418, 118th Cong. (2023).

⁷⁵ 89 Fed. Reg. 2034, 2066 (Jan. 11, 2024).

serve as a “written children’s data retention policy”⁷⁶ for purposes of the proposed requirement, so long as it satisfies all of the requirements described in the Rule and extends to children’s personal information. The final Rule should not adopt the proposed requirement that operators state the “business need for retaining” personal information, which is redundant with the required statement of purpose.

Moreover, the FTC should give operators reasonable flexibility to determine whether and where retention information is presented on their websites and services, rather than requiring that it be provided as part of the online notice. While operators should maintain and implement internally a data retention policy, publishing such policies online would needlessly lengthen and complicate privacy notices with no meaningful benefit to parents. Where operators choose to voluntarily publish data retention schedules, this information may be more useful if provided in just-in-time disclosures or customer support articles, rather than in the privacy policy. Such an approach could provide transparency where useful to consumers and avoid redundancy where an operator already discloses retention information elsewhere on the website or service.

In keeping with this streamlined approach, the FTC also should align the retention policy language with state privacy laws, which generally do not require publication of specific retention timeframes. For example, California law permits publication of “the criteria used to determine that [retention] period provided that a business shall not retain a consumer’s personal information . . . for longer than is reasonably necessary for [each] disclosed purpose [for which the information was collected].”⁷⁷

The FTC also should clarify the NPRM’s proposed position that children’s personal information may only be retained as long as is necessary for the business purpose for which it was collected. For example, it is unclear whether an operator’s use of personal information to improve its products and services constitutes a “secondary” purpose for which data may not be retained. It is also unclear whether using information originally collected to show a child the correct piece of content to personalize content subsequently shown to the child would constitute a secondary purpose. The FTC has recognized that using personal information for purposes of product improvement and personalization is beneficial for consumers and should be encouraged through the “support for internal operations” exception.⁷⁸ It similarly should facilitate such activities by specifying that activities constituting “support for internal operations” are not “secondary purposes.”⁷⁹

For these reasons, we urge the FTC to further revise the proposed Rule as follows:

⁷⁶ 89 Fed. Reg. 2034, 2075 (Jan. 11, 2024)

⁷⁷ Cal. Civ. Code § 1798.100(a)(3).

⁷⁸ *See, e.g.*, 16 C.F.R. § 312.2 (including “personaliz[ing] the content on[] the Web site, or online service” within the support for internal operations exception).

⁷⁹ A strict definition of “secondary purposes” for retained data collected with parental consent could also raise First Amendment concerns by making it more difficult for operators to provide users with access to requested lawful content.

An operator of a website or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the specific purpose(s) for which the information was collected and **to provide support for the internal operations of the website or online service,** not for a secondary purpose. **A purpose is a secondary purpose if it does not advance the operator’s ability to effectuate its original purpose or otherwise relate closely to the original purpose.** When such information is no longer reasonably necessary for the purpose for which it was collected, the operator must delete the information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion. Personal information collected online from a child may not be retained indefinitely. At a minimum, the operator must establish, implement, and maintain a written children’s data retention policy that sets forth the purposes for which children’s personal information is collected, ~~the business need for retaining such information,~~ and a timeframe for deletion of such information that precludes indefinite retention. The operator must provide its written children’s data retention policy **on the website or online service in a manner that is reasonably conspicuous to parents; provided that in lieu of the specific timeframe, the operator may state the criteria used to determine when data must be deleted. in the notice on the website or online service provided in accordance with section § 312.4(d).**⁸⁰

VIII. The FTC Should Clarify that an Existing Security Program can Satisfy the NPRM’s Proposed Children’s Data Security Program Requirement.

The NPRM proposes requiring that operators “establish, implement, and maintain a written comprehensive security program” that includes elements such as annual risk assessments and safeguards that reflect the sensitivity of children’s personal information.⁸¹ However, it is unclear whether operators with an existing comprehensive security program must implement a *separate* children’s data security program, including by designating an employee coordinator and implementing safeguards and risk assessments specific to children.

Requiring that operators implement a separate children’s data security program misunderstands the holistic nature of data security and may create unnecessarily redundant and unduly burdensome work where an operator’s existing comprehensive data security program already considers the sensitivity of all data processed by the operator, including children’s data. This redundancy has no additional benefit for consumers. The additional recordkeeping involved in implementing a children’s data security program could raise concerns under the Paperwork Reduction Act, particularly if operators are required to provide granular assessments of potential risks to children’s data. Based on our experience, the NPRM’s estimates regarding the amount of time that it will likely take operators to comply with new recordkeeping requirements — including risk assessments — are much lower than could be expected in practice. Implementing and documenting a compliant children’s data security program will take most operators a substantial amount of time depending on the number and complexity of an operator’s websites and services.

⁸⁰ 89 Fed. Reg. 2034, 2075 (Jan. 11, 2024).

⁸¹ 89 Fed. Reg. 2034, 2075 (Jan. 11, 2024)

To minimize Paperwork Reduction Act concerns and accelerate operators' implementation efforts, the FTC should modify the proposed Rule to clarify that a generally applicable comprehensive data security program will be in compliance with the proposed requirement if it addresses the sensitivity of personal information, including information collected from children. Specifically, Section 312.8(b) of the proposed Rule should be revised as follows:

At a minimum, the operator must establish, implement, and maintain a written children's personal information security program that contains safeguards that are appropriate to the sensitivity of the personal information collected from children and the operator's size, complexity, and nature and scope of activities. **An operator with a comprehensive written data security program may satisfy this requirement by ensuring that such program meets the requirements described below.** To establish, implement, and maintain a children's personal information security program, the operator must: [. . .]

IX. Any Interpretation Regulating Personal Information That is not Collected Directly "From" a Child Would Exceed the FTC's Statutory Authority.

The NPRM proposes to delete the word "directly" from the second paragraph of the Rule's definition of a "website or online service directed to children," which currently reads "[a] website or online service shall be deemed directed to children when it has actual knowledge that it is collecting personal information *directly* from users of another website or online service directed to children."⁸²

This approach would expand the definition of a website or online service "directed to children" beyond what COPPA's statutory text allows. The FTC's 2013 interpretation already stretches the bounds of the FTC's statutory authority by conflating the two distinct prongs of 15 U.S.C. § 6502(a)(1), actual knowledge and child-directedness. The statute is explicit that "actual knowledge" triggers COPPA's requirements only where such knowledge is of collection "from a child."⁸³ Actual knowledge of another service's child-directedness is not equivalent to actual knowledge of collection from a specific child. Moreover, the statutory definition of a website or service directed to children makes no reference to "actual knowledge," and instead depends entirely on whether the operator's website or service is targeted to children.⁸⁴

Deleting the word "directly" as described above would push the Rule's definition of a website or service "directed to children" even further from the language of the statute. The proposed definition would improperly render superfluous the statutory requirement that collection

⁸² 16 C.F.R. § 312.2.

⁸³ 15 U.S.C. § 6502(a)(1) ("It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information *from* a child . . .") (emphasis added).

⁸⁴ 15 U.S.C. § 6501(10).

be “from a child.” For that reason, it would be even more susceptible to challenge than the FTC’s 2013 interpretation.

The proposed Rule also would, in effect, require a recipient of personal information to assess the COPPA status of all vendors from which it receives such data. This is not only impractical, but it exceeds the bounds of the statute enacted by Congress: nothing in the statute suggests that a business should be transitively responsible for data processing decisions made by other businesses. Compliance would become particularly difficult when vendors rebrand or launch new products or services that could change their status under COPPA. Recipients of personal information would have to continually assess their third-party partners, a burdensome and imprecise exercise. At present, there is no established means by which operators could put other businesses on notice of their COPPA status (and changes thereto).

It is also unclear how a business that collects personal information directly from another corporate entity, rather than from the child, could go about providing parents notice and securing verifiable parental consent in practice, particularly for those elements of the COPPA Rule’s “personal information” definition that do not themselves actually permit physical or online contacting. For example, a recipient receiving only persistent identifiers or photos containing a child’s image cannot use this information to contact the child or the child’s parent to provide notice and obtain consent. The Commission should avoid such interpretations that produce impossible, absurd, or impractical results.

Even where it would be possible for a business to satisfy the notice and consent requirements (because, for example, they receive an email address), the revised Rule would provide no meaningful benefits for parents. The operator who collected the personal information directly from the child already would be required to provide parents notice and obtain consent for its disclosure of personal information to third parties under COPPA. Interpreting COPPA to also require businesses who collect personal information from other corporate entities (instead of directly from the child) to provide notice and obtain consent would only subject parents to a deluge of overlapping and redundant notices and requests for consent. Because the business receiving the personal information from the operator has no direct relationship with the child or their parent, parents likely would find this outreach confusing and overly complicated.

X. The FTC Rightly Concluded Text Messages can be a Valid Method of Obtaining Verifiable Parental Consent.

We support the FTC’s conclusion that sending a text message to parents should be a valid method of obtaining verifiable parental consent. Permitting parents to provide consent via text message is consistent with COPPA’s legislative intent, which encourages the use of *any* reasonable consent mechanism, based on available technology. Today, parents regularly use text messaging to communicate, to sign up for services, and to authenticate their identity. Expanding the list of recognized parental consent mechanisms to recognize this option would offer parents significant convenience and utility.

While the text of the proposed COPPA Rule helpfully updates the definition of “online contact information” to include mobile phone numbers, we urge the FTC to make a corresponding

change to explicitly recognize consent via a parental text message as a pre-approved mechanism for obtaining verifiable parental consent. The NPRM suggests this isn't needed due to the update to the "online contact information" definition. However, because none of the pre-approved mechanisms for verifiable parental consent refer specifically to "online contact information," additional clarity would be helpful. Specifically, Section 312.5(b) of the COPPA Rule, which lists the pre-approved verifiable parental consent mechanisms, does not reference the term "online contact information," and therefore changes to the definition of that term are not incorporated by reference. For the avoidance of doubt, the Commission should revise Section 312.5(b)(2) as follows:

(b) *Methods for verifiable parental consent.*

...

(2) Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include:

(i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan;

(ii) Requiring a parent, in connection with a transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

(iii) Having a parent call a toll-free telephone number staffed by trained personnel;

(iv) Having a parent connect to trained personnel via video-conference;

(v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete;

...

(ix) Having a parent reply to a message sent using the parent's online contact information; or ...

XI. Operators Should Only Need to Secure New Verifiable Parental Consent for a new Feature Where There was a Material Change in the Operator's Data Processing Practices.

The NPRM suggests a clarification to Section 312.5(a)(1) of the Rule, which requires that an operator obtain VPC "before any collection, use, or disclosure of personal information from children," including when the operator modifies practices to which a parent had previously consented. The NPRM seeks to clarify that the VPC requirement "applies to any *feature* on a

website or online service through which an operator collects personal information from a child” (emphasis added).

Unfortunately, the NPRM’s statement creates ambiguity rather than resolving it, and must be further clarified. Specifically, we understand the FTC did not intend to require operators to seek VPC every time a new feature is introduced, even when prior notices and consent covers such processing of the child’s personal information. Such an interpretation would be inconsistent with the text of the COPPA Rule, which states explicitly that additional verifiable parental consent is required only for “any material change in the collection, use, or disclosure” of the child’s personal information. It also would be detrimental to parents, who would face a deluge of consent requests from websites and services seeking to implement new features with no meaningful changes in how their child’s information is processed.

To avoid this ambiguity, the FTC should clarify that it was merely re-iterating what the COPPA Rule already requires – that verifiable parental consent must be updated when there are material changes in how an operator collects, uses, or discloses personal information from children. Relatedly, the FTC also should re-iterate its longstanding guidance that verifiable parental consent can be updated through, for example, a password or PIN number that the operator uses to confirm the parent’s identity in any future contact with them.⁸⁵

XII. The FTC Should Provide Operators Time to Come into Compliance with the new Rule Requirements.

The FTC appropriately recognizes that there will need to be a delayed effective date for modifications to the Rule introduced by this proceeding. However, the FTC should extend the proposed effective date to two years.

If operators are required to obtain verifiable parental consent for the first time for activities that previously did not require such consent, operators will need significant time to provide parents with notice and permit parents time to consent. For example, many operators currently collect only user name or screen name without verifiable parental consent, because they do not use this information as online contact information. Under the proposed COPPA Rule, these operators now may need to obtain verifiable parental consent to continue allowing the child to access the service. If parents are provided too little time to respond to requests to provide verifiable parental consent, they might be surprised if their child’s access to functionality or the services is terminated (particularly if the parent paid for such access or content, such as in-app purchases).⁸⁶

Moreover, if age estimation provisions are enacted, operators will need sufficient time to conduct the analysis required to assess whether they qualify for the exception. If, at the end of the assessment, the evidence suggests they are not a general audience service, such operators would

⁸⁵ Fed. Trade Comm’n, COPPA FAQ I.8, <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>.

⁸⁶ 15 U.S.C. § 6502(b)(3)(permitting operators to terminate the service where a parent does not provide verifiable parental consent).

need to come into compliance as a child-directed service for the first time, requiring additional time.


Many of the proposed changes, if enacted, would require significant modifications not only to notices and documentation, but also to how websites and services are engineered. To comply with the modifications, operators would have to both redesign user interfaces and disclosures and complete the extensive reengineering work and testing required to implement these changes prior to the effective date. Planning for budgets and resources for significant re-engineering efforts can require a year or more of lead time.

Notably, other laws that have required significant design changes or compliance assessments, such as the EU General Data Protection Regulation, provided a two-year period to come into compliance.⁸⁷ Accordingly, we urge the FTC to provide at least two years for operators to come into compliance with the new requirements.

* * *

IAB thanks the Commission for this opportunity to submit these comments and looks forward to working closely with the Commission on this important topic. Please do not hesitate to contact me at lartease@iab.com with any questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Lartease Tiffith", with a long horizontal flourish extending to the right.

Lartease M. Tiffith, Esq.
Executive Vice President for Public Policy
Interactive Advertising Bureau

⁸⁷ GDPR Art. 99 (adopted April 14, 2016, entered into force on May 25, 2018).