8 March 2024

Response by the Centre for Information Policy Leadership to the FTC's Notice of Proposed Rulemaking on the Children's Online Privacy Protection Rule

COPPA Rule Review, Project No. P195404

Submitted March 8, 2024

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the Notice of Proposed Rulemaking (NPRM)[2] by the Federal Trade Commission regarding its implementation of the Children's Online Privacy Protection Act (COPPA) through amendments to the Children's Online Privacy Protection Rule (COPPA Rule or Rule).

TABLE OF CONTENTS

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Children's Online Privacy Protection Rule Notice of Proposed Rulemaking, 89 FR 2034, Jan. 11, 2024 (hereinafter "FTC COPPA Rule NPRM"), available at https://www.federalregister.gov/documents/2024/01/11/2023-28569/childrens-online-privacy-protection-rule.

I. Comments on Expanding the COPPA Rule's Coverage

A. "Website or Online Service Directed to Children"

CIPL supports the Commission's decision not to modify the Rule's definition of "website or online service directed to children." We agree that the adoption of a per se legal standard—specifically, that a website should be deemed "directed to children" if audience demographics show that a certain percentage or more of its visitors are children under age 13—is unnecessary. We agree with the Commission's conclusion that it already considers the demographics of a website's or online service's user base in its determination; a per se legal standard is not needed, nor would it be advisable. We also support the Commission's decision not to expand the definition to cover sites and services "likely to attract" an audience that includes a disproportionately large percentage of children under age 13, given that such a standard is too vague absent further clarification.[3]

That said, the NPRM invites further comment on whether the Commission should provide an exemption under which an operator's site or service would not be deemed "directed to children" if the operator undertakes an analysis of the site's or service's audience composition and determines that no more than a specific percentage of its users are likely to be children under 13 years of age. The Commission views the proposed exemption as an "incentive to encourage operators to conduct an analysis of their sites' or services' user bases."[4]

As the Commission itself notes, the definition of "website or online service directed to children" already permits the Commission to consider "competent and reliable empirical evidence regarding audience composition,"[5] and the COPPA Rule already sets forth a multi-factor test for determining whether a website or online service, or a portion thereof, is directed to children. While CIPL generally supports regulations that incentivize organizations to adopt best practices, we urge the Commission to consider carefully any potential impact that adoption of this incentive could have on the multi-factor test, as the exemption would highlight a single factor (audience composition) to the exclusion

---

3 FTC COPPA Rule NPRM, 89 FR 2034, 2036.

4 *Id.*

5 16 CFR § 312.2.

of other factors. CIPL queries whether the proposed exemption introduces a mixed message regarding the multi-factor test and whether it could effectively establish a per se legal standard, which the Commission has already rejected.

B. "Actual Knowledge" Standard

We commend the Commission for deciding to retain the COPPA Rule's "actual knowledge" standard. As noted in our response[6] to the FTC's 2019 Request for Comment (2019 Rule Review), the Commission must ensure that any amendments to the Rule stay within its statutory boundaries. The statutory text refers to "actual knowledge,"[7] and the Commission correctly concludes that Congress did not intend "actual knowledge" to include the concept of constructive knowledge.

C. Rebuttable Presumption

CIPL agrees that operators of child-directed sites and services must presume that their users are children. In the context of general audience platforms, however, where third parties upload child-directed content, operators should be given the opportunity to rebut the presumption that all users of such content are children. Our 2019 Response[8] stated as much: the COPPA Rule should consider reasonable measures adopted by platform operators (such as age-gating with additional verification) to ensure that users interacting with that content are not under 13 years of age.

The Commission, however, has decided not to permit general audience platforms to rebut the presumption, noting in particular that "the reality of parents and children sharing devices, along with account holders remaining perpetually logged into their accounts, could make it difficult for an operator to distinguish reliably between those users who are children and those who are not."[9] Moreover, the Commission notes that, with its newly proposed definition of "mixed audience" websites and services, the COPPA Rule will essentially allow operators to rebut the presumption as to the users of a subset of child-directed sites and services that do not target children as their primary audience.

We agree with the Commission that the mixed audience category affords operators an appropriate degree of flexibility, as it would not preclude an operator from taking reasonable steps to ensure that users interacting with the child-directed content on its platform are 13 or older.

---

[6] CIPL Response to the FTC's Implementation of the Children's Online Privacy Protection Rule, Dec. 11, 2019 (hereinafter, "CIPL 2019 Response"), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_the_ftcs_coppa_consultation_12.11.2019.pdf.

[7] 15 USC § 6502(a)(1) (providing that "[i]t 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, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b)"). Emphasis added.

[8] CIPL 2019 Response, *supra*, note 5.

[9] FTC COPPA Rule NPRM, 89 FR at 2039.

II. Comments on Proposed Modifications

A. Definitions

1. Online Contact Information

The Commission proposes to amend "online contact information" by adding "an identifier such as a mobile telephone number provided the operator uses it only to send a text message." This modification would allow operators to collect and use a parent's or child's mobile phone number in certain circumstances, including in connection with obtaining parental consent through a text message.[10]

CIPL supports the expansion of methods to secure parental consent, including via text message, but the Commission should provide further guidance on how such an exchange would be carried out in practice. For example, would operators of child-directed sites and services need to verify whether the mobile telephone number provided by a child is, in fact, the parent's number?

2. Personal Information

a. Biometric Data

The Commission also proposes to modify the Rule's definition of "personal information" to include "[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."[11]

As CIPL noted in our 2019 Response,[12] it is important for the Commission to formulate rules in a manner that facilitates interoperability with international and existing U.S. laws and not to hinder innovation. The proposed inclusion of the term "biometric identifier" can cause confusion because it is not a term that is commonly used in laws and regulations that target biometric systems. CIPL's forthcoming white paper on biometric technology[13] will highlight inconsistencies among and between laws in the U.S. and beyond, and how these inconsistencies can cause uncertainty and frustrate compliance. CIPL recommends that terminology and definitions related to biometric technology be aligned with standards organizations, like the International Organization for Standardization (ISO), which does not use the term "biometric identifier" in its publication that seeks to standardize information technology vocabulary concerning biometric systems.[14] The Commission's proposed use of the term "biometric identifier" will unnecessarily drive confusion and uncertainty among organizations. CIPL therefore recommends use of the term "biometric data" to align with other laws addressing this topic.

Since the proposal will modify the Rule's definition of "personal information," the Commission should clarify that biometric data is only personal information when it is intended to be used for identification

---

[10] *Id.*, at 2040.

[11] *Id.*, at 2041.

[12] CIPL 2019 Response, *supra*, note 5.

[13] CIPL will provide the Commission with a copy of the white paper once published.

[14] International Standards Organization. (2022-23). *Information technology — Vocabulary — Part 37: Biometrics*. (ISO/IEC2382-37), available at https://www.iso.org/standard/73514.html.

purposes. Thus, CIPL asks the Commission to change "can be used" to "will be used," as it is important for the intent requirement to consider whether operators have taken reasonable measures (e.g., technical, organizational, and contractual) to ensure that the processing of biometric characteristics is—or is not—intended to be used for identifying purposes. Further, while CIPL supports the Commission's listing of specific kinds of biometric characteristics, we suggest language such as "includes but is not limited to ..." to clarify the intended scope of the provision.

b. Inferred and Other Data

CIPL commends the Commission for deciding not to expand the Rule's definition of "personal information" to include data that is inferred about, but not directly collected from, children, or other data that serves as a proxy for "personal information." As the Commission correctly notes, COPPA expressly pertains to the collection of personal information *from* a child.[15]

The Commission notes, however, that inferred data or data that may serve as a proxy for "personal information" could nevertheless fall within the Rule's scope where it is combined with additional data that would meet the Rule's current definition of "personal information." CIPL would like greater clarification from the Commission on this point. The so-called "catch-all" provision references "information concerning the child or the parents of that child that the operator collects online *from the child*."[16] Since the Commission has already stated that inferred data does not fall within the scope of the Rule because it is not collected "from a child," the Commission should clarify how inferred data would nevertheless fall within the scope of the catch-all provision and provide assurance that the internal operations exception would not be compromised.

c. Persistent Identifiers

CIPL has no comment on the Commission's decision to retain "persistent identifiers" in the Rule's definition of "personal information," but it asks the Commission to clarify whether inferred data falls within the definition of "persistent identifiers."

3. School and School-Authorized Education Purpose

CIPL's comments on the Commission's decision related to Education Technology are addressed in Section II.C.3.a, *infra*.

4. Support for the Internal Operations of the Website or Online Service

The COPPA Rule recognizes an exception to the notice and consent requirements for operators that collect a persistent identifier for the "sole purpose of providing support for the internal operations of the website or online service."[17] The Rule defines "support for the internal operations of the website or online service" to include a number of specified activities, but it also includes an important use restriction: the information collected to perform those activities cannot be used or disclosed "to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose."[18]

---

[15] 15 USC § 6502(a)(1).

[16] 16 CFR § 312.2

[17] 16 CFR § 312.5(c)(7).

[18] 16 CFR § 312.2.

CIPL supports the Commission's proposal to add the clause "*Provided, however, that, except as specifically permitted by paragraphs 1(i) through(vii) of this definition"* to the use restriction,[19] as it clarifies that information collected for the specified support activities may be used or disclosed to carry out those enumerated activities. For additional clarity, CIPL encourages the Commission to expand on the enumerated activities—especially activities necessary to "maintain or analyze the functioning of the website or online service"—by making reference to the specific practices mentioned in the preamble to the Commission's 2013 amendments,[20] as well as to the specific practices identified in the current NPRM, such as ad attribution[21] and contextual advertising.[22]

CIPL, however, requests greater clarity on the Commission's proposal to add the clause "*in connection with processes that encourage or prompt use of a website or online service*.[23] The phrase "encourage or prompt use" is not defined and could unwittingly prohibit innovative and beneficial uses for end users, such as links to online resources cited as references or provided for users to learn more about a related topic. CIPL would support a more tailored use restriction that would not block legitimate and beneficial use cases or create a broad prohibition on certain design choices.

CIPL also has concerns about the Commission's proposal to modify the internal operations exception by way of an amendment to the Rule's online notice requirement. The proposal would require any operator using the internal operations exception to specifically identify in its online notice the

---

[19] As proposed, the text would be amended as follows: "[~~So long as~~] *Provided, however, that, except as specifically permitted by paragraphs 1(i) through(vii) of this definition,* the information collected for the activities listed in paragraphs (1)(i) [–] *through* (vii) of this definition [~~is not~~] *cannot be* used or disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, *in connection with processes that encourage or prompt use of a website or online service,* or for any other purpose."

[20] "The Commission declines to add certain other language proposed by commenters, such as intellectual property protection, payment and delivery functions, spam protection, optimization, statistical reporting, or de-bugging, because it believes that these functions are sufficiently covered by the definitional language permitting activities that 'maintain or analyze' the functions of the Web site or service, or protect the 'security or integrity' of the site or service." Children's Online Privacy Protection Rule, 78 FR 3972, 3981 (Jan. 17, 2013), available at https://www.federalregister.gov/documents/2013/01/17/2012-31341/childrens-online-privacy-protection-rule.

[21] "The Commission believes that ad attribution, where a persistent identifier is used to determine whether a particular advertisement led a user to take a particular action, falls within various categories, such as the concept of 'payment and delivery functions' and 'optimization and statistical reporting.' When used as a tool against click fraud, ad attribution also falls within the category of 'protecting against fraud or theft,' an activity that served as a basis for the Commission's creation of the support for the internal operations exception." FTC COPPA Rule NPRM, 89 FR at 2045.

[22] "[I]t bears noting, as the Commission did in 2013, that the expansion of the personal information definition was coupled with a newly created exception that allows operators to collect persistent identifiers from children to provide support for the internal operations of the website or online service without providing notice or obtaining parental consent. One of these purposes is serving contextual advertising, which provides operators another avenue for monetizing online content. The Commission continues to believe that it struck the proper balance in 2013 when it expanded the personal information definition while also creating a new exception to the Rule's requirements." FTC COPPA Rule NPRM, 89 FR at 2043.

[23] The proposed text reads in part: "information collected [under the internal operations exemption] cannot be used or disclosed … in connection with processes that encourage or prompt use of a website or online service …" FTC COPPA Rule NPRM, 89 FR at 2072.

practices for which it has collected a persistent identifier and the means it uses to comply with the use restriction.[24]

While CIPL is supportive of transparency measures, we seek guidance on how the disclosure of such practices could be conveyed in such a way as to be useful, since internal operations are usually quite technical. Moreover, such disclosures could potentially reveal confidential information, security measures, proprietary information, and trade secrets. CIPL encourages the Commission to consider such matters before finalizing the proposed amendment.

5. Website or Online Service Directed to Children

a. Multi-Factor Test

CIPL agrees that the Rule's multi-factor test,[25] which applies a "totality of the circumstances" standard, is the most practical and effective means for determining whether a website or online service is directed to children. CIPL supports the Commission's proposal to add an operator's "marketing or promotional materials or plans, representations to consumers or to third parties" to the non-exhaustive list of examples of evidence for consideration in analyzing audience composition and intended audience.

However, CIPL does not support adding "reviews by users or third parties, and the age of users on similar websites or services" to the list of examples without further clarification. It is not clear how such reviews would be authenticated as genuine, and the Commission does not state how the "age of users" would be determined or measured, or how a given website or service would be deemed "similar."

b. Operators Collecting Personal Information from Other Websites and Online Services Directed to Children

The Commission proposes to modify the second paragraph of the definition of "website or online service directed to children" by deleting the word "directly":

> [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.

Here, the Commission is concerned that entities "with actual knowledge that they receive large amounts of children's data from another site or service that is directed to children, without collecting it directly from the users of such site or service" may avoid COPPA's requirements.[26]

---

[24] FTC COPPA Rule NPRM, 89 FR at 2045.

[25] "In determining whether a Web site or online service, or a portion thereof, is directed to children, the Commission will consider its subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the Web site or online service, as well as whether advertising promoting or appearing on the Web site or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience." 16 CFR § 312.2.

[26] FTC COPPA Rule NPRM, 89 FR at 2047.

The Commission should take into consideration the practical implications for compliance resulting from the proposed expansion of this provision, including how a recipient can assess whether the initial collection of children's data was done in compliance with COPPA (i.e., whether the initial site or service properly secured parental consent to disclose the child's data to third parties), or how a recipient shall satisfy the notice and consent requirements absent a direct relationship with the child or parent (or even the site or service that initially collected the data).

c. Mixed Audience

The Commission proposes adding to the Rule a separate, stand-alone definition for "mixed audience website or online service":

> *Mixed audience website or online service* means a website or online service that is directed to children under the criteria set forth in paragraph (1) of the definition of website or online service directed to children, but that does not target children as its primary audience, and does 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. 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 or encourage visitors to falsify age information.[27]

While CIPL commends the Commission for attempting to clarify the obligations for a mixed audience website or online service, the proposed definition could be clearer.

CIPL suggests the following definition:

> *Mixed audience website or online service* means a website or online service that does not target children as its primary audience but where a portion of the website or online service would satisfy the criteria set forth in paragraph (1) of the definition of website or online service directed to children.

CIPL then proposes to amend paragraph (3) of the definition of "website or online service directed to children" by stating:

> (3) A mixed audience website or online service shall not be deemed directed to children if it employs measures that are reasonably calculated, considering available technology, to determine that visitors are 13 years of age or older. The measures used to determine whether visitors are 13 years old or older should be proportionate to the level of harm being addressed or avoided by the methodology.

The Commission's proposed requirement to collect age information "in a neutral manner that does not … encourage visitors to falsify age information" presents considerable challenges.

Age assurance methodologies currently available to organizations—including self-declaration models, AI-powered age-estimation approaches, biometrics-based tools, and third-party provider services—present different levels of accuracy and different levels of privacy-invasiveness. Some are more privacy-protective, while others require the collection of personal information for the specific age

[27] FTC COPPA Rule NPRM, 89 FR at 2071.

verification or assurance purpose. Arguably their use could deter internet usage, raising potential First Amendment concerns.

Choosing a specific methodology requires an assessment of the risks and benefits of different methods, such as whether it would require the collection of additional personal information. The assessment should also consider whether the impact of a given methodology is proportionate to the level of harm being addressed or avoided by the methodology. For example, choosing an age *verification* tool where age *estimation* would suffice might require disproportionate collection of personal data. Identifying the most appropriate method means balancing its effectiveness with privacy protections.

The Commission should recognize the need for operators to perform a risk/benefit assessment before choosing a particular methodology. In some low-risk situations, a self-declaration of age may be sufficient, even though visitors may be able to falsify age information. The Commission should clarify that an operator's decision to use a methodology that cannot preclude falsification does not mean that the operator "*encourage[s]* visitors to falsify age information."

B. Notice

1. Direct Notice to the Parent

CIPL supports the Commission's proposal to add references to "school" in 16 CFR § 312.4(b) to cover the situation in which an operator relies on authorization from a school to collect information from a child and provides the direct notice to the school rather than to the child's parent.

2. Content of the Direct Notice

The Commission's proposed modifications to § 312.4(c) are substantial.

First and foremost, the proposed change to the first sentence greatly expands the scope of the provision. As currently drafted, § 312.4(c) sets forth the required content of the direct notice when an operator collects personal information to initiate parental consent under the parental consent exception listed in § 312.5(c)(1). The proposed modification would clarify that the direct notice requirement applies to *all instances* in which the operator provides direct notice to a parent for the purposes of obtaining consent, not just for the parental consent exception under § 312.5(c)(1).

The proposed amendment to subparagraph (c)(iii) would require disclosure of not only *what* personal information the operator intends to collect from the child, but also "*how* the operator *intends to use* such information."[28] To avoid any ambiguity concerning *how* the operator intends to use personal information, CIPL would support instead a requirement to disclose the **purpose** for which the data will be used. A purpose requirement is present in many privacy laws, and it would be reasonable to include one here.

The proposed addition of new subparagraph (c)(iv) would also require the operator to disclose the *identities or specific categories of third parties* to whom personal information is disclosed as well as the *purposes* for such disclosures. While CIPL supports a requirement calling for the disclosure of *categories of third parties* and of the *purposes* for such disclosures, we wanted the Commission to be aware that the disclosure of the ***identities of third parties*** could prove to be challenging for some

[28] FTC COPPA Rule NPRM, 89 FR at 2073 (emphasis added).

businesses, as the identities of third parties may be subject to frequent change. That said, we appreciate the Commission's use of the conjunction "or" to make the disclosure of identities optional.

New subparagraph (c)(iv) would further require the operator to provide notice that parents can consent to the collection and use of the child's personal information without consenting to the disclosure to third parties (except where such disclosure is "integral to the nature of the website or online service"). CIPL's comments regarding this change—which will require operators to obtain separate verifiable parental consent—are addressed in Section II.C.1., *infra*.

As for the proposed addition of new subparagraph (c)(5)—which identifies the content of the direct notice when seeking school authorization to collect personal information (and which largely tracks the content required when seeking parental consent)—CIPL highlights the same concerns: (1) rather than an explanation of *how* the operator *intends to use* personal information,[29] CIPL would support instead a requirement to disclose the **purpose** for which the data will be used; and (2) while a requirement calling for the disclosure of *categories of third parties* or of the *purposes* for such disclosures would be reasonable, disclosure of the ***identities of third parties*** could prove to be challenging for some businesses and should remain optional.[30]

3. Notice on the Website or Online Service

The Commission proposes two additions and certain modifications to the Rule's existing online notice requirements.

First, the Commission proposes adding a new subparagraph (d)(3), which would require operators that collect a persistent identifier under the support for the internal operations exception in § 312.5(c)(7) to identify the "specific internal operations" for which the operator has collected the persistent identifier and describe the "means [it] uses to ensure" that it does not use or disclose the persistent identifier to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, in connection with processes that encourage or prompt use of a website or online service, or for any other purpose, except as permitted by the support for the internal operations exception.[31] As noted above in our comments to the internal operations exception,[32] CIPL is supportive of transparency measures, but we would appreciate the Commission's guidance on how the disclosure of such practices could be conveyed in such a way as to be useful, since internal operations are usually

---

[29] As proposed, 16 CFR § 321.4(c)(5)(iii) would require the direct notice to schools to set forth "[t]he items of personal information the operator intends to collect from the child, how the operator intends to use such information, and the potential opportunities for the disclosure of personal information, should the school provide authorization…." FTC COPPA Rule NPRM, 89 FR at 2073.

[30] As proposed, 16 CFR § 321.4(c)(5)(iv) would require the direct notice to schools to include "the identities or specific categories of such third parties and the specific school-authorized education purposes for such disclosure …." FTC COPPA Rule NPRM, 89 FR at 2073.

[31] As proposed, 16 CFR § 321.4(d)(3) would say: "If applicable, the specific internal operations for which the operator has collected a persistent identifier pursuant to § 312.5(c)(7); and the means the operator uses to ensure that such identifier is not used or disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, in connection with processes that encourage or prompt use of a website or online service, or for any other purpose (except as specifically permitted to provide support for the internal operations of the website or online service) …." FTC COPPA Rule NPRM, 89 FR at 2074.

[32] See Section II.A.4, *supra*.

quite technical. Moreover, such disclosures could potentially reveal confidential information, security measures, proprietary information, and trade secrets.

For example, one activity covered by the internal operations exception would include operators' efforts to protect "the security and integrity of the user, website, or online service." Read broadly, the proposed disclosure obligations could require operators to reveal previously nonpublic security practices, which bad actors could exploit. 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 could be able to tailor attacks to circumvent the system. CIPL encourages the Commission to consider such matters before finalizing the proposed amendment.

Second, the Commission proposes adding a new subparagraph (d)(4) to require an operator that collects audio files pursuant to the new § 312.5(c)(9) exception to describe how the operator uses the audio files and to represent that it deletes such files immediately after responding to the request for which the files were collected.[33] As mentioned in other contexts, CIPL would support clarification that the Commission seeks disclosure of the **purpose** for which the data will be used rather than technical explanations of *how* the operator uses audio files.

Third, the Commission proposes modifying subparagraph (d)(2) to require additional information regarding operators' disclosure practices and operators' retention policies, "including the identities or specific categories of any third parties to which the operator discloses personal information and the purposes for such disclosures; and the operator's data retention policy as required under § 312.10 …."[34] As mentioned above in the context of the direct notice,[35] CIPL supports a requirement calling for the disclosure of *categories of third parties* and of the *purposes* for such disclosures, but disclosure of the ***identities of third parties*** could prove to be challenging for some businesses, as the identities of third parties may be subject to frequent change. That said, we appreciate the Commission's use of the conjunction "or" to make the disclosure of identities optional. As for the data retention policy, see CIPL's comments in Section II.F., *infra*.

The Commission notes that the Rule's online notice provision already requires operators to describe *how* they use personal information collected from children.[36] As such, the Commission claims that an operator is already required to disclose, for example, whether it uses personal information "to encourage or prompt use of the operator's website or online service such as through a push notification."[37] CIPL, however, does not view that sort of disclosure to be intuitive to a requirement to disclose *how* personal information is used. Rather, whether personal information is used "to encourage or prompt use" seems to respond to the question of *why*, or *for what purpose,* rather than

---

[33] As proposed, 16 CFR § 321.4(d)(4) would say: "Where the operator collects audio files containing a child's voice pursuant to § 312.5(c)(9), a description of how the operator uses such audio files and that the operator deletes such audio files immediately after responding to the request for which they were collected …" FTC COPPA Rule NPRM, 89 FR at 2074.

[34] FTC COPPA Rule NPRM, 89 FR at 2073-74.

[35] Section II.B.2., *supra*.

[36] In pertinent part, 16 CFR § 321.4(d)(2) provides that the online notice must state … "[a] description of what information the operator collects from children..; how the operator uses such information; and, the operator's disclosure practices for such information…"

[37] FTC COPPA Rule NPRM, 89 FR at 2050.

how. As stated earlier,[38] to avoid any ambiguity concerning *how* the operator intends to use personal information, CIPL would support a requirement to disclose the **purpose** for which it will be used.

Moreover, as stated earlier,[39] "encourage or prompt use" is not defined and could unwittingly prohibit innovative and beneficial uses for end users, such as links to online resources cited as references or provided for users to learn more about a related topic. If the Commission seeks disclosure regarding practices that "encourage or prompt use," the Commission should draft a tailored definition that would not block legitimate and beneficial use cases.

C. Parental Consent

1. General Requirements

The Commission seeks to clarify that the verifiable parental consent requirement applies to *any feature* on a website or online service through which an operator collects personal information from a child. It further proposes to amend the verifiable parental consent requirement by requiring operators to obtain *separate verifiable parental consent* for disclosures of a child's personal information, unless such disclosures are integral to the nature of the website or online service.[40]

Disaggregating consent may be desirable and even warranted in certain use cases. For example, if the sharing of data with third parties is not necessary for the operation of a site, disaggregating the consents may be consistent with the expectation that companies do not condition participation in an activity on greater data collection than is necessary. However attempting to secure multiple consents could negatively impact the user experience and risk contributing to consent fatigue, which ultimately lowers privacy protections with reflexive box ticking instead of informed decision-making. Furthermore, it could degrade the quality of users' experience where, for example, parents may be required to enter the same information twice in rapid succession.

---

[38] See Section II.A.4., *infra*.

[39] *Id.*

[40] As proposed, § 312.5(a)(2) would say: "An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties, unless such disclosure is integral to the nature of the website or online service. An operator required to give the parent this option must obtain separate verifiable parental consent to such disclosure, and the operator may not condition access to the website or online service on such consent." FTC COPPA Rule NPRM, 89 FR at 2074.

Given the limitations of notice and consent as repeatedly acknowledged by FTC officials,[41] CIPL's comments to the Commission's ANPR on Commercial Surveillance and Data Security[42] remain relevant here:

> Consent is often regarded as a desirable, easy-to-use ground for processing personal data that gives choice to individuals. In practice, however, consent can be cumbersome, transient, and both overwhelming and meaningless for individuals who face a barrage of requests without the time, inclination, or capacity to review them to the level required for informed decision making. Consent can also be difficult to collect, as it must often meet certain standards to be considered valid.[43]

Admittedly, the Commission's authority to act is constrained by COPPA's notice-and-consent framework, but additional notice-and-consent requirements could discourage parents from reviewing notices that provide meaningful information. The Commission should take these factors into consideration to permit a more flexible approach that addresses when and to what extent a separate notice would be warranted.

2. Methods for Verifiable Parental Consent

CIPL supports the Commission's proposed modifications to the Rule's parental consent provisions: (1) eliminating the monetary transaction requirement when an operator obtains consent through a parent's use of a credit card, debit card, or an online payment system;[44] (2) permitting the use of text messages to obtain consent; and (3) adding two parental consent methods to § 312.5(b)—specifically, knowledge-based authentication and the use of facial recognition technology.

---

[41] The Commission itself has recognized the limitations of the notice-and-consent framework. See Trade Regulation Rule on Commercial Surveillance and Data Security, FTC Advance Notice of Proposed Rulemaking, 87 FR 51273, 51287, available at https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security (emphasis added). Chair Khan has voiced her concern that "market realities" may render the notice-and-consent paradigm "outdated and insufficient." Remarks of Chair Lina M. Khan as Prepared for Delivery IAPP Global Privacy Summit 2022, April 11, 2022, available at https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks%20of%20Chair%20Lina%20M.%20Khan%20at%20IAPP%20Global%20Privacy%20Summit%202022%20-%20Final%20Version.pdf. Commissioner Slaughter has similarly described the notice-and-consent model as being "outdated." Statement of Commissioner Rebecca Kelly Slaughter, Opening Remarks at PrivacyCon 2021, July 27, 2021, available at https://www.ftc.gov/system/files/documents/public_statements/1592854/slaughter_statement_privacycon_7-27-21.pdf. Director Levine has gone so far as to characterize the notice-and-choice regime as a fiction. Remarks of BCP Director Samuel Levine at 2023 Consumer Data Industry Association Law & Industry Conference, September 21, 2023, available at https://www.ftc.gov/system/files/ftc_gov/pdf/cdia-sam-levine-9-21-2023.pdf.

[42] CIPL Response to the FTC's ANPR on Commercial Surveillance and Data Security, November 21, 2022, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_ftc%E2%80%99s_anpr_on_commercial_surveillance_and_data_security_21_nov_2022_.pdf.

[43] *Id.*, p. 50.

[44] Of course, the Commission should recognize that credit card processors may not agree to have their gateways used for zero-charge transactions.

3. Exceptions to Prior Parental Consent

a. School Authorization Exception

CIPL generally supports the Commission's proposal to create a school authorization exception, but we seek additional clarification regarding the "person providing authorization" and the attestation that "the person has the authority to do so."[45] For example, where an individual teacher wishes to use a particular provider's services, could the teacher qualify as a "person providing authorization," with a department head or school administrator providing the attestation? Must each school or school district establish a written policy documenting the chain of command for authorization and attestation? Will the Commission provide a sample written agreement for providers to apply? May schools use terms from clickwrap agreements, or must they undergo a more robust contracting process that retains greater school autonomy?

Moreover, we encourage the Commission to collaborate with the Department of Education to ensure that the Rule's proposed school authorization exception will align with the "school official exception" in the Family Educational Rights and Privacy Act (FERPA).[46] Greater clarity in the Rule or joint guidance from the Commission and the Department of Education is likely necessary to ensure that schools and EdTech vendors comply with both FERPA and COPPA. Moreover, it would be helpful for the Commission to ensure that its proposed product development exception does not conflict with state student privacy laws, especially those following the Student Online Personal Information Protection Act (SOPIPA) model.[47] Unintended preemption issues should be avoided.

D. Prohibition Against Conditioning a Child's Participation on Collection of Personal Information

Section 312.7 of the Rule provides that an operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity. The Commission is considering including language in § 312.7 to provide that an "activity" means "any activity offered by

---

[45] As proposed, § 12.5(c)(10) would provide:

> Where the operator obtains school authorization for the collection of the child's personal information for a school-authorized education purpose. In such a case, the operator must ensure that the school receives notice as described in § 312.4(c)(5) and must have a written agreement with the school that:
>
> (i) Indicates the name and title of the person providing authorization and attests that the person has the authority to do so;
>
> (ii) Limits the operator's use and disclosure of the personal information to a school-authorized education purpose only and no other purpose;
>
> (iii) Provides that the operator is under the school's direct control with regard to the use, disclosure, and maintenance of the personal information collected from the child pursuant to school authorization; and
>
> (iv) Sets forth the operator's data retention policy with respect to such information in accordance with § 312.10.

FTC COPPA Rule NPRM, 89 FR at 2075.

[46] 20 USC § 1232g (b)(1)(A).

[47] Student Online Personal Information Protection Act, available at https://publicleadershipinstitute.org/model-bills/civil-rights-liberties/student-online-personal-information-protection-act-sopipa/.

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."[48]

CIPL recommends that the Commission define "activity" with greater clarity to lower the risk of blocking legitimate and beneficial use cases, and also to avoid inadvertently excluding activities that should not be excluded. For example, the Commission may wish to clarify whether an activity "offered" by a website or online service should always be understood as being "a subset or component" of the website or online service, or whether some activities might be deemed "offered" but not "a subset or component," such as giveaways of physical prizes.

E. Confidentiality, Security, and Integrity of Personal Information Collected From Children

The Commission proposes modifications to the Rule's security requirements, notably by requiring operators to establish, implement, and maintain a written comprehensive security program that contains safeguards that are appropriate to the sensitivity of children's information and to the operator's size, complexity, and nature and scope of activities.[49]

CIPL agrees that operators should put in place safeguards for data appropriate for the sensitivity of children's information—and indeed, appropriate to the sensitivity of all data. Thus, CIPL does not believe that operators should necessarily be required to establish, implement, and maintain security programs specifically tailored to children's personal information. As the Commission itself acknowledges, its proposal is modeled on the Safeguards Rule implemented under the Gramm-Leach-

---

[48] FTC COPPA Rule NPRM, 89 FR at 2059-60.

[49] As proposed, § 312.8(b) would provide:

> 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. To establish, implement, and maintain a children's personal information security program, the operator must:
>
> (1) Designate one or more employees to coordinate the operator's children's personal information security program;
>
> (2) Identify and, at least annually, perform additional assessments to identify internal and external risks to the confidentiality, security, and integrity of personal information collected from children and the sufficiency of any safeguards in place to control such risks;
>
> (3) Design, implement, and maintain safeguards to control risks identified through the risk assessments required under paragraph (b)(2) of this section. Each safeguard must be based on the volume and sensitivity of the children's personal information that is at risk, and the likelihood that the risk could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information;
>
> (4) Regularly test and monitor the effectiveness of the safeguards in place to control risks identified through the risk assessments required under paragraph (b)(2) of this section; and
>
> (5) At least annually, evaluate and modify the children's personal information security program to address identified risks, results of required testing and monitoring, new or more efficient technological or operational methods to control for identified risks, or any other circumstances that an operator knows or has reason to know may have a material impact on its children's personal information security program or any safeguards in place.

FTC COPPA Rule NPRM, 89 FR at 2075.

Bliley Act ("GLBA").[50] Consequently, operators who are financial institutions already have such programs in place. The Commission should acknowledge situations where similar requirements already exist and are already being met by operators. To the extent operators already have a comprehensive security program in place, the need for a separate program addressing children's personal information would be unnecessary. Instead, the Commission could ask operators to document practices under existing security programs that adequately protect children's personal information.

Moreover, the Commission's proposal to require the designation of "one or more employees" as the coordinator of a children's information security program[51] risks being redundant with existing CISO designations required by other laws, regulations, and/or industry standards that are already on the books. If the Commission preserves this requirement, it should clarify that the coordinator role can be assigned to an information security professional within the context of their broader duties.

F. Data Retention and Deletion Requirements

The Commission proposes to amend the Rule's data retention and deletion requirements to prohibit operators from retaining children's personal information indefinitely, and to require operators to 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.[52]

While CIPL understands the Commission's concerns regarding the indefinite retention of data, the Rule should make allowances for specific use cases that may warrant indefinite retention. For example, operators of online gaming services may need to keep certain data indefinitely in accordance with users' expectations. Users expect gaming platforms to remember their scores, interactions, purchases, communications, and other transactions indefinitely. In other cases, users may let an account lapse, but reactivate it later with the expectation of accessing prior history. Operators should therefore have the flexibility to retain information for use cases where retention would make sense.

Moreover, the Rule should recognize situations where an operator has collected data for a specific purpose, and the operator no longer needs the data for that purpose, but the operator must nevertheless retain the data to comply with other laws or regulations. Compliance with such legal obligations would arguably constitute a "secondary purpose," which the Commission's proposed text would prohibit. The Commission should clarify that a "secondary purpose" would not encompass

---

[50] FTC COPPA Rule NPRM, 89 FR at 2016.

[51] See § 312.8(b), as proposed, FTC COPPA Rule NPRM, 89 FR at 2075.

[52] As proposed, § 312.10 would provide: "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 not for a secondary 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 in the notice on the website or online service provided in accordance with § 312.4(d)." FTC COPPA Rule NPRM, 89 FR at 2075.

common exemptions—such as for security, fraud prevention, financial recordkeeping, legal and regulatory requirements, ensuring service continuity, and consent for extended retention of data.

G. Safe Harbor

1. Criteria for Approval of Self-Regulatory Program Guidelines

To the extent the Commission's proposed modifications to the Rule's security requirements (discussed in Section II.E., *supra*) offer guidance to its criteria for approving the self-regulatory guidelines of an FTC-approved COPPA Safe Harbor program, CIPL raises the same concerns. Approval of self-regulatory guidelines should not be conditioned on a requirement to establish a security program specifically tailored to children's personal information. To the extent the guidelines recognize a provider's establishment of a comprehensive security program, there is no need for an FTC-approved COPPA Safe Harbor program to require a separate security program addressing children's personal information.

However, CIPL supports the Commission's proposed modification to § 312.11(b)(2), which states that an FTC-approved COPPA Safe Harbor program's assessments of subject operators must include comprehensive reviews of both the subject operators' *privacy and security* policies, practices, and representations. [53]

2. Reporting and Recordkeeping Requirements

The Commission proposes to require FTC-approved COPPA Safe Harbor programs to identify each subject operator and all approved websites or online services in the program, as well as all subject operators that have left the program.[54] The Commission proposes to add a new § 312.11(f) requiring FTC-approved COPPA Safe Harbor programs to submit triennial reports that provide details about

---

[53] "An effective, mandatory mechanism for the independent assessment of subject operators' compliance with the self-regulatory program guidelines. At a minimum, this mechanism must include a comprehensive review by the safe harbor program, to be conducted not less than annually, of each subject operator's information privacy and security policies, practices, and representations." 16 CFR § 312.11(b)(2), as proposed, FTC COPPA Rule NPRM, 89 FR at 2076.

[54] 16 CFR § 312.11(d)(1), as proposed, would provide:

> By [DATE SIX MONTHS AFTER PUBLICATION OF THE FINAL RULE IN THE FEDERAL REGISTER], and annually thereafter, submit a report to the Commission that identifies each subject operator and all approved websites or online services, as well as any subject operators that have left the safe harbor program. The report must also contain, at a minimum:
>
> (i) A narrative description of the safe harbor program's business model, including whether it provides additional services such as training to subject operators;
>
> (ii) Copies of each consumer complaint related to each subject operator's violation of a safe harbor program's guidelines;
>
> (iii) An aggregated summary of the results of the independent assessments conducted under paragraph (b)(2) of this section;
>
> (iv) A description of each disciplinary action taken against any subject operator under paragraph (b)(3) of this section, as well as a description of the process for determining whether a subject operator is subject to discipline; and
>
> (v) A description of any approvals of member operators' use of a parental consent mechanism, pursuant to § 312.5(b)(4);

programs' technological capabilities and mechanisms for assessing subject operators' fitness for maintaining membership.[55] The Commission also proposes to require that FTC-approved COPPA Safe Harbor programs publish lists of their subject operators.[56]

CIPL supports the Commission's proposed modifications.

3. Revocation of Approval of Self-Regulatory Program Guidelines

CIPL supports the Commission's proposal to update existing statutory language that reserves the Commission's right to revoke the approval of any FTC-approved COPPA Safe Harbor program whose guidelines or implementation of guidelines do not meet the requirements set forth in the Rule.[57]

H. Voluntary Commission Approval Processes

CIPL has no objection to the Commission's proposed modifications.[58]

---

[55] "Every three years approved safe harbor programs shall submit to the Commission a report detailing the safe harbor program's technological capabilities and mechanisms for assessing subject operators' fitness for membership in the safe harbor program." 16 CFR § 312.11(f), as proposed, FTC COPPA Rule NPRM, 89 FR at 2076.

[56] 16 CFR § 312.11(d)(1), as proposed.

[57] "The Commission reserves the right to revoke any approval granted under this section if at any time it determines that the approved self-regulatory program guidelines or their implementation do not meet the requirements of this part." 16 CFR § 312.11(g), as proposed, FTC COPPA Rule NPRM, 89 FR at 2076.

[58] "An interested party may file a written request for Commission approval of additional activities to be included within the definition of support for the internal operations of the website or online service. To be considered for approval, a party must provide a detailed justification why such activities should be deemed support for the internal operations of the website or online service, and an analysis of their potential effects on children's online privacy. The request shall be filed with the Commission's Office of the Secretary. The Commission will publish in the **Federal Register** a document seeking public comment on the request. The Commission shall issue a written determination within 120 days of the filing of the request." 16 CFR § 312.12(b), as proposed.