Billing Code: 6750-01-P

FEDERAL TRADE COMMISSION

16 CFR Part 312

RIN 3084–AB20

Children's Online Privacy Protection Rule

AGENCY: Federal Trade Commission.

ACTION: Final rule amendments.

SUMMARY: The Federal Trade Commission amends the Children's Online Privacy Protection Rule, consistent with the requirements of the Children's Online Privacy Protection Act. The amendments to the Rule, which are based on the FTC's review of public comments and its enforcement experience, include a new definition for *Mixed audience website or online service* and modifications to the definitions of *Disclose or disclosure*, *Online contact information*, *Operator, Personal information*, *Support for the internal operations of the website or online service*, *Third party*, and *Website or online service directed to children*, as well as updates to key provisions to respond to changes in technology and online practices. The amendments are intended to strengthen protection of personal information collected from children, and, where appropriate, to clarify and streamline the Rule since it was last amended in January 2013.

DATES:

Effective date: The amended Rule is effective [INSERT DATE THAT IS 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

Compliance date: Except with respect to § 312.11(d)(1), (d)(4), and (g), regulated entities have until [INSERT DATE THAT IS 365 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*] to comply.

ADDRESSES: The complete public record of this proceeding will be available at *www.ftc.gov*.

FOR FURTHER INFORMATION CONTACT: James Trilling, Attorney, (202) 326-3497; Manmeet Dhindsa, Attorney, (202) 326-2877; Elizabeth Averill, Attorney, (202) 326-2993; Andy Hasty, Attorney, (202) 326-2861; or Genevieve Bonan, Attorney, (202) 326-3139, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, DC 20580.

STATEMENT OF BASIS AND PURPOSE

I. Overview and Background

A. Overview

This document states the basis and purpose for the Federal Trade Commission's ("Commission" or "FTC") decision to adopt certain amendments to the Children's Online Privacy Protection Rule that were proposed and published for public comment on January 11, 2024 in a notice of proposed rulemaking ("2024 NPRM").[1] After careful review and consideration of the entire rulemaking record, including public comments submitted by interested parties, and based upon its enforcement experience, the Commission has determined to adopt amendments to the Children's Online Privacy Protection Rule, 16 CFR 312 ("COPPA Rule" or "Rule"). These amendments will update and clarify the COPPA Rule, consistent with the requirements of the Children's Online Privacy Protection Act ("COPPA" or "COPPA statute"), 15 U.S.C. 6501 et seq., to protect children's personal information and give parents control over their children's personal information.

The final amendments to the COPPA Rule include a new definition for *Mixed audience website or online service* that is intended to provide greater clarity regarding an existing sub-

[1] Children's Online Privacy Protection Rule, Notice of Proposed Rulemaking, 89 FR 2034 (Jan. 11, 2024), available at *https://www.govinfo.gov/content/pkg/FR-2024-01-11/pdf/2023-28569.pdf*.

category of child-directed websites and online services under the Rule. The final amendments also modify the definitions of *Online contact information* to include mobile telephone numbers; *Personal information* to include government-issued identifiers and biometric identifiers that can be used for the automated or semi-automated recognition of an individual; *Support for the internal operations of the website or online service* to clarify that information collected for the enumerated activities in the definition may be used or disclosed to carry out those activities; and *Website or online service directed to children* to provide some examples of evidence the Commission may consider in analyzing audience composition and intended audience, and to adjust the third paragraph to align with the new definition of *Mixed audience website or online service.* In addition, the Commission is modifying operators' obligations with respect to direct and online notices; information security, deletion, and retention protocols; and FTC-approved COPPA Safe Harbor programs' annual assessment, disclosure, and reporting requirements. The Commission is also adopting amendments related to parental consent requirements, methods of obtaining verifiable parental consent, and exceptions to the parental consent requirement. The Commission is replacing the term "web site" with "website" throughout the Rule and making other minor stylistic or grammatical changes to the Rule that the Commission proposed in the 2024 NPRM.

In the 2024 NPRM, the Commission proposed a number of Rule modifications relating to educational technology ("ed tech"), including new definitions of *School* and *School-authorized education purpose*,[2] as well as provisions governing collection of information from children in schools,[3] and codifying a school authorization exception to obtaining verifiable parental

[2] 89 FR 2034 at 2043-2044.
[3] *Id.* at 2053-2058, 2059.

consent.[4] In Fall 2024, the United States Department of Education ("DOE") affirmed its intention to propose amendments to the Family Educational Rights and Privacy Act ("FERPA") regulations, 34 CFR 99, "to update, clarify, and improve the current regulations by addressing outstanding policy issues, … and clarify[] provisions governing non-consensual disclosures of personally identifiable information from education records to third parties."[5] These changes may be relevant to provisions of the COPPA Rule related to ed tech and school authorization that the Commission proposed in the 2024 NPRM. To avoid making amendments to the COPPA Rule that may conflict with potential amendments to DOE's FERPA regulations, the Commission is not finalizing the proposed amendments to the Rule related to ed tech and the role of schools at this time.[6] The Commission will continue to enforce COPPA in the ed tech context consistent with its existing guidance.[7]

B. Background

Congress enacted COPPA in 1998. On November 3, 1999, the Commission issued the COPPA Rule, which became effective on April 21, 2000.[8] The COPPA Rule imposes certain requirements on operators of websites[9] or online services directed to, or with actual knowledge

---

[4] *Id*. The Commission also asked a question about what types of services should be considered to have an educational purpose. *Id.* at 2071 (Question 16).
[5] Department of Education Fall 2024 Unified Agenda, RIN: 1875-AA15, available at *https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202410&RIN=1875-AA15*.
[6] This approach is consistent with that taken in a prior Commission rulemaking. *See* Energy Labeling Rule, Final rule, 87 FR 61465, 61466 (Oct. 12, 2022), available at *https://www.federalregister.gov/documents/2022/10/12/2022-22036/energy-labeling-rule* ("In response to comments, the Commission will wait to update television ranges until [the Department of Energy] completes proposed test procedure changes for those products.").
[7] *See Complying with COPPA: Frequently Asked Questions* ("COPPA FAQs"), FAQ Section N, available at *https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions*; FTC, *Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act* (May 19, 2022), available at *https://www.ftc.gov/legal-library/browse/policy-statement-federal-trade-commission-education-technology-childrens-online-privacy-protection*. The Commission will monitor and weigh future developments with respect to DOE's potential FERPA regulation amendments in deciding whether to pursue COPPA Rule amendments related to ed tech.
[8] Children's Online Privacy Protection Rule, Final rule, 64 FR 59888 (Nov. 3, 1999), available at *https://www.federalregister.gov/documents/1999/11/03/99-27740/childrens-online-privacy-protection-rule*.
[9] *See* 89 FR 2034 at 2040 for discussion of the Commission's change from using the term "Web site" to "website" throughout the Rule.

of the collection of personal information from, children under 13 years of age (collectively, "operators"). The Rule requires that operators provide direct and online notice to parents and obtain verifiable parental consent before collecting, using, or disclosing personal information from children under 13 years of age.[10] Additionally, the Rule requires operators to provide parents the opportunity to review the types of personal information collected from their child, delete the collected information, and prevent further use or future collection of personal information from their child.[11] The Rule requires operators to keep personal information they collect from children secure and to maintain effective data retention and deletion protocols for that information.[12] The Rule prohibits operators from conditioning children's participation in activities on the collection of more personal information than is reasonably necessary to participate in such activities.[13] The Rule also includes a "safe harbor" provision that allows industry groups or others to submit to the Commission for approval self-regulatory guidelines that implement the Rule's protections.[14]

In 2013, the Commission adopted changes to the COPPA Rule, consistent with the COPPA statute, in light of changing technology and business practices ("2013 Amendments").[15] Subsequent changes in how children utilize online services led the Commission to propose in January 2024, and now to finalize, further additional revisions to the COPPA Rule to enable COPPA to continue to meet its goal of protecting children online.

The Commission initiated the underlying review of the COPPA Rule in July 2019 when it published a document in the *Federal Register* seeking public comment about the Rule's

[10] 16 CFR 312.3, 312.4, and 312.5.
[11] 16 CFR 312.3 and 312.6.
[12] 16 CFR 312.8 and 312.10.
[13] 16 CFR 312.7.
[14] 16 CFR 312.11.
[15] *See* Children's Online Privacy Protection Rule, Final Rule Amendments, 78 FR 3972 (Jan. 17, 2013), available at *https://www.federalregister.gov/documents/2013/01/17/2012-31341/childrens-online-privacy-protection-rule*.

application to the ed tech sector, voice-enabled connected devices, and general audience platforms that host third-party child-directed content ("2019 Rule Review Initiation").[16] In response to the 2019 Rule Review Initiation, the Commission received more than 175,000 comments from a variety of stakeholders, including industry representatives, content creators, consumer advocacy groups, academics, technologists, FTC-approved COPPA Safe Harbor programs, members of Congress, and other individual members of the public.

Following consideration of these comments and other feedback received, the Commission issued the 2024 NPRM in the *Federal Register* on January 11, 2024.[17] The Commission received 279 unique responsive comments.[18] After carefully reviewing these additional comments, the Commission now announces this final amended COPPA Rule.

II. Modifications to the Rule

A. Stylistic, Grammatical, and Punctuation Changes

In the 2024 NPRM, the Commission proposed minor revisions to the Rule to address various stylistic, grammatical, and punctuation issues. The Commission proposed amending the Rule to change the term "Web site" to "website" throughout the Rule, noting that this better aligns with the COPPA statute's use of the term, as well as how the term is used in the marketplace.[19] The Commission also proposed amending § 312.1 of the Rule to adjust the location of a comma.[20] The Commission proposed two technical fixes to § 312.5(c)(6) that

[16] *See* Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 84 FR 35842 (July 25, 2019), available at *https://www.federalregister.gov/documents/2019/07/25/2019-15754/request-for-public-comment-on-the-federal-trade-commissions-implementation-of-the-childrens-online*.
[17] 89 FR 2034.
[18] Public comments filed in response to the 2024 NPRM are available at *https://www.regulations.gov/docket/FTC-2024-0003/comments*.
[19] 89 FR 2034 at 2040. The Statement of Basis and Purpose incorporates this change in all instances in which the current Rule uses the term "Web site."
[20] *Id.* at 2040.

included adjusting § 312.5(c)(6)(i) to "protect the security or integrity of *the* website or online service" and removing the word "be" in § 312.5(c)(6)(iv) to fix a typographical error in the current Rule.[21] The Commission additionally proposed making a few edits in § 312.12(b) to ensure that each reference to the support for the internal operations of the website or online service is consistent with the COPPA statute's use of the phrase "support for the internal operations of the [website] or online service."[22] The Commission did not receive any feedback from commenters regarding these minor changes and adopts them in the final Rule.[23]

B. Section 312.2: Definitions

1. Definition of "Mixed Audience Website or Online Service"

a. The Commission's Proposal Regarding "Mixed Audience Website or Online Service"

The Commission proposed a new stand-alone definition for "mixed audience website or online service" as "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."[24] The proposed definition further requires that "[a]ny 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

[21] *Id.* at 2059 (emphasis added).
[22] *Id.* at 2064, 2076.
[23] Additionally, the final Rule will include in § 312.5(b)(viii), after "Provided that," a comma that appears in the current Rule but was inadvertently omitted from the proposed Rule text in the 2024 NPRM. The final Rule will also include in § 312.5(d)(4), before the phrase "for each such operator," a comma that was inadvertently omitted from the proposed Rule text in the 2024 NPRM.
[24] 89 FR 2034 at 2071.

a set age or encourage visitors to falsify age information."[25] The Commission explained in the 2024 NPRM that this proposed stand-alone definition is intended to make clearer in the Rule the existing category for "mixed audience" websites and online services under the Rule and to provide greater clarity about the means by which operators of mixed audience sites and services can determine whether a user is a child.[26]

Since the Commission established the "mixed audience" category in the 2013 Amendments, the Commission has viewed "mixed audience" sites and services as a subset of the "child-directed" category of websites or online services.[27] Under both the current and the proposed amended Rule, a website or online service can fall under the mixed audience designation if it is: (1) "child-directed" under the Rule's multi-factor test, and (2) does not target children as its primary audience.[28] The new definition does not change the established two-step analysis used to determine whether a website or online service is mixed audience.[29] The threshold inquiry under the existing Rule and the proposed new definition for "mixed audience website or online service" is whether a website or online service is directed to children, based on an evaluation of the factors set forth in the first paragraph of the definition of "website or online

[25] *Id.*
[26] *Id*. at 2048.
[27] 78 FR 3972 at 3983-84. Staff guidance has also addressed this category. *See* COPPA FAQs, FAQ Section D.4.
[28] When codifying this approach in 2013, the Commission noted that it would first apply the "totality of the circumstances" standard set forth in paragraph (1) of the definition of website or online service directed to children to determine whether the site or service is directed to children, and then the Commission would determine whether children are the primary audience for the site or service. 78 FR 3972 at 3984.
[29] Many commenters responding to the 2024 NPRM asked the Commission to clarify whether the determination of whether a site or service is mixed audience remains a two-step process or whether the Commission is changing that process with the new definition and related changes to the definition of "website or online service directed to children." *See, e.g.*, U.S. Chamber of Commerce ("Chamber"), at 7; Entertainment Software Association ("ESA"), at 7; Interactive Advertising Bureau ("IAB"), at 12-13. The Commission has carefully considered alternative definitions proffered by these and other commenters, but believes the proposed definition is sufficiently clear about the relevant two-step analysis for identifying mixed audience websites and online services. The Commission reiterates its earlier guidance related to the second step of the analysis, that it "intends the word 'primary' to have its common meaning, *i.e.*, something that stands first in rank, importance, or value," and that this will be determined by considering the totality of the circumstances and not through a precise audience threshold. *See* 78 FR 3972 at 3984 n.162.

service directed to children." If a website or online service is directed to children under that analysis, then the second step in the determination of whether a website or online service is "mixed audience" is to ask whether it targets children as its primary audience. Both steps of the analysis require consideration of a totality of the circumstances and the factors set forth in the first paragraph of the definition of "website or online service directed to children."

Unlike other child-directed sites and services, those that do not target children as their primary audience may decide to age screen visitors in order to apply COPPA's protections only to visitors who identify as under 13. Under both the current Rule and proposed stand-alone definition for "mixed audience website or online service," an operator of a mixed audience website or online service may not collect personal information from any visitor until it collects age information from the visitor or uses another means that is reasonably calculated, in light of available technology, to determine whether the visitor is under 13. To the extent that a visitor identifies as under 13, the operator may not collect, use, or disclose the child's personal information without first complying with the Rule's notice and parental consent provisions.

b. Public Comments Received in Response to the Commission's Proposal Regarding "Mixed Audience Website or Online Service"

The proposed stand-alone definition of "mixed audience website or online service" received general support from many commenters, but also generated many requests for clarification.[30] For example, some commenters asked whether the new definition is intended to expand the scope of child-directed websites and online services.[31] It is not. The Commission reiterates that mixed audience websites and online services are a subset of child-directed

[30] *See, e.g.*, Children and Screens: Institute of Digital Media and Child Development ("Children and Screens"), at 6; Google, at 3; Information Technology Industry Council ("ITIC"), at 4-5; kidSAFE Seal Program ("kidSAFE"), at 7.
[31] *See, e.g.*, ITIC, at 4-5; ACT | The App Association, at 5.

websites and online services, and the proposed definition of "mixed audience website or online service" does not change which websites or online services are directed to children under the Rule.

A number of commenters asked for additional guidance about when websites and online services will be considered general audience, primarily child-directed, or mixed audience.[32] The Commission directs these commenters to earlier staff guidance, which explains that operators should analyze who their intended audience is, who their actual audience is, and the likely audience of their website or online service and consider the multiple factors identified in the first paragraph of the Rule's definition of "website or online service directed to children."[33]

Other commenters expressed concern that the new definition prevents mixed audience websites and online services from utilizing the exceptions to the COPPA Rule's verifiable parental consent requirement set forth in § 312.5(c).[34] In response, the Commission clarifies that operators of mixed audience websites and online services may utilize the exceptions to the verifiable parental consent requirement set forth in § 312.5(c) of the Rule, as is true for operators of child-directed websites and online services targeting children as their primary audience. The Commission is also adding language to the definition of "mixed audience website or online service" to clarify this issue by stating that operators of such websites and online services may not "collect personal information from any visitor, other than for the limited purposes set forth in § 312.5(c), prior to collecting age information or using another means…to determine whether the visitor is a child."

---

[32] Google, at 3 (supporting adding a stand-alone definition for mixed audience website or online service, but stating that "further clarity is needed on the distinction between a general audience service or mixed audience service that 'does not target children as its primary audience' and a primarily child-directed service"); The Toy Association, Inc. ("The Toy Association"), at 4-5 (contending that distinction between "primarily" and "secondarily" directed to children is not clear).

[33] *See* COPPA FAQs, FAQ Sections D.1, D.3, and D.5.

[34] *See, e.g.*, ESA, at 7; IAB, at 12-13.

One commenter urged the Commission to state that general audience and mixed audience websites and online services containing "kid-friendly portions" of content or services are not primarily child-directed.[35] This request for clarification is somewhat unclear, as it is not apparent to the Commission what the commenter means by "kid-friendly portions." If a portion of a general audience website or online service is directed to children, then the operator must treat all visitors to that portion of the website or online service as children.[36] If a portion of a general audience website or online service is directed to children but does not target children as its primary audience, the operator can choose to age screen visitors to that portion and must comply with COPPA obligations with respect to visitors identified as under 13. Another industry commenter contended that a general audience website or online service "should not become a mixed audience property just because the property does not include mature content and is presented as appropriate for children."[37] In response, the Commission notes that it agrees that a general audience website or online service, or portion thereof, is not necessarily child-directed merely because it includes content that is appropriate for children and reiterates that categorization is determined by evaluating the totality of the circumstances and the multiple factors set forth in the definition of "website or online service directed to children."

Another commenter suggested amending the definition of "mixed audience website or online service" to mean "a website or online service that does not target children as its primary

[35] *See* Google, at 3. The commenter further suggested "[a]bsent clear guidance on this issue, companies may choose not to offer kid-friendly experiences or content on their service due to the risk of the entire service being deemed primarily child-directed." *Id*. Somewhat similarly, another industry commenter asked the Commission to clarify that general audience websites and online services will not be deemed to be mixed audience just because they "host pockets of child-directed content" and that such guidance is essential to "forestall general audience services from making a Hobson's choice between age gating all users or removing children's content from among their offerings." NCTA – The Internet and Television Association ("NCTA"), at 10-11.

[36] The statutory definition of "website or online service directed to children" includes "that portion of a commercial website or online service that is targeted to children." 15 U.S.C. 6501(10)(A)(ii). The definition of "Web site or online service directed to children" in the Rule also clearly establishes that a portion of a website or online service may be child-directed. 16 CFR 312.2.

[37] Privacy for America, at 7.

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."[38] However, a portion of a website or online service may be primarily directed to children even if the website or online service as a whole is not. The Commission thus declines to amend the definition of "mixed audience website or online service" in response to this comment.

The proposed definition of "mixed audience website or online service" also included language to provide additional clarity about how an operator of a mixed audience website or online service can determine whether a user is a child. The Commission received a variety of comments about this aspect of the proposed definition. Some commenters expressed support for the flexibility built into the Commission's proposal to permit operators of mixed audience websites or online services to collect age information or use other reasonably calculated means to determine whether a visitor is a child.[39]

Other commenters raised concerns related to this aspect of the proposed definition of "mixed audience website or online service." For example, one commenter opposed references to the "collection of age information" on the ground that "collection" implies retention of information, which the commenter indicated should not be necessary to achieve the goal of determining users' ages; the commenter favored alternative age verification strategies that avoid retention of age information.[40] In response, the Commission notes that it disagrees that

[38] Centre for Information Policy Leadership ("CIPL"), at 8. The Commission declines to adjust the proposed definition in this way and believes that it would result in confusion.
[39] *See, e.g.*, kidSAFE, at 7 (expressing support for inclusion of language allowing for other methods of age gating to provide clarity and spur innovation); Google, at 3 (expressing support for flexibility and suggesting the proposed change "will allow companies to leverage new and emerging age verification mechanisms"). In the 2024 NPRM, the Commission observed that the proposed language "allows operators to innovate and develop additional mechanisms that do not rely on a user's self-declaration." 89 FR 2034 at 2048.
[40] Internet Safety Labs, at 6-7.

collection of age information necessarily requires retention of the exact age of a visitor or user,[41] or that operators' retention of information that a user is 12 years old, or 40 years old, would violate the Rule. Another commenter argued the Commission should require the use of "privacy-protected age estimation methods to determine the likely age of users" rather than including an age verification requirement that would require additional personal data collection and management.[42] Other commenters suggested the Rule should require additional methods of verification when operators of mixed audience websites or online services are relying on self-declarations to determine whether the visitor is a child.[43] The Commission does not have adequate evidence from the record to assess potential benefits and burdens associated with these alternative proposals and declines to amend the definition to impose additional verification obligations on operators at this time.

Other commenters requested clarification about whether the proposed definition of "mixed audience website or online service" permits collection of information without first obtaining parental consent for the purpose of determining whether a user is a child.[44] In response, the Commission notes that most of these commenters do not specify the type of information they contemplate operators collecting to determine age or what identifiers such information might be combined with. However, one industry commenter requested that the Commission consider an exception in the Rule allowing operators to collect personal information such as photographs to estimate a visitor's age as "another means" to determine age under the

[41] For example, one commenter suggested operators could retain a Boolean of "user age under 13: Y/N." Internet Safety Labs, at 7.
[42] *See* Electronic Privacy Information Center ("EPIC"), at 5.
[43] *See, e.g.*, Motley Rice, at 13 (suggesting Commission should require COPPA-compliant measures to corroborate self-declarations of age because of falsification risks).
[44] *See, e.g.*, ITIC, at 4-5; ACT | The App Association, at 5; Consumer Technology Association, at 2. *See also* Google, at 3-4 (requesting exception from COPPA obligations when personal information is collected solely to verify a user's age using alternative age verification methods); Network Advertising Initiative ("NAI"), at 7 (same).

proposed definition of "mixed audience website or online service" without triggering COPPA compliance obligations.[45] The Commission did not propose such an exception to the COPPA Rule's verifiable parental consent requirement in the 2024 NPRM and did not intend to propose one when adding the provision for "another means that is reasonably calculated in light of available technology" to the definition of "mixed audience website or online service." The Commission reiterates that the COPPA Rule applies to "personal information" collected online from children.[46] To the extent operators collect information to determine whether a visitor is a child from sources other than a child, such as from a reliable third-party platform, this would not be considered collection of "personal information" under the Rule.

Another commenter suggested that the neutrality requirement for age screening in the proposed definition "presents considerable challenges" because age assurance methodologies present different levels of accuracy and some require the collection of personal information for age assurance while others do not.[47] The commenter further suggested the Rule should require operators to select an age assurance methodology based on the risks and benefits of different methods, as well as whether the privacy impact of a specific methodology is proportionate to the

[45] Google, at 4. ("[W]e believe additional protections are needed for companies that use alternative methods to age-screen users. Under the existing Rule, date of birth is not considered 'personal information.' This allows companies to collect date of birth from users in order to age-screen those users without triggering compliance obligations under the Rule. We believe the same protection should apply to other categories of information that may be collected to age-screen users under the revised Rule. For example, using selfies for age verification to estimate a user's age (in a privacy-preserving manner, and without identifying them) may become a more reliable age verification method than asking users to provide their age. Under the current Rule, however, this would be unworkable, as photos containing a child's image constitute 'personal information,' and collecting a selfie from a user under 13 would thus trigger compliance obligations.").

[46] *See* 16 CFR 312.3.

[47] *See* CIPL, at 8-9. In response, the Commission notes that it did not intend for the requirement that collection or other means of determining whether a visitor is a child "must be done in a neutral manner" to require that the means used must be neutral with respect to associated risks and benefits. Instead, the Commission included this provision to make clear that collection or other means employed to age screen visitors must not guide visitors to a particular age or encourage them to indicate they are over the age of 12 through design choices, nudges, communications or site content, or in other ways. Staff guidance has previously addressed this concern. *See* COPPA FAQs, FAQ Section D.7.

level of harm being addressed or avoided by the methodology.[48] The Commission believes the proposed definition provides sufficient guidance and flexibility for operators to select from age assurance methodologies and declines to incorporate the suggested harm-based calculation into the Rule. The Commission agrees with commenters expressing the view that it is important to allow operators to innovate and develop alternative, improved mechanisms to determine age that do not rely on a visitor's self-declaration and finds that the proposed language best accomplishes this.

c. The Commission Adopts Amendments Regarding "Mixed Audience Website or Online Service"

After carefully considering the record and comments, and for the reasons discussed in Part II.B.1.b of this document, the Commission is adopting an amended version of the proposed definition of "mixed audience website or online service" that includes additional language clarifying operators of mixed audience websites and online services may collect personal information for the limited purposes set forth in § 312.5(c) prior to determining visitor age. The Commission intends for operators of mixed audience websites and online services to have the same ability to utilize the exceptions to the verifiable parental consent requirement set forth in § 312.5(c) as operators of other child-directed websites and online services.

2. Definition of "Online Contact Information"

a. The Commission's Proposal Regarding "Online Contact Information"

In the 2024 NPRM, the Commission proposed amending the definition of "online contact information" in § 312.2 of the Rule by adding to the non-exhaustive list of identifiers that

[48] *See* CIPL, at 8-9.

constitute online contact information "an identifier such as a mobile telephone number provided the operator uses it only to send a text message."[49] The Commission proposed this amendment to allow operators to collect and use a parent's or child's mobile phone number in certain circumstances, including in connection with using a text message to initiate the process of seeking verifiable parental consent.[50] The proposed amendment was intended to give operators another way to initiate the process of seeking parental consent quickly and effectively.

b. Public Comments Received in Response to the Commission's Proposal Regarding "Online Contact Information"

A substantial majority of commenters addressing the proposed amendment to the definition supported it.[51] Supporters suggested that permitting operators to utilize text messages to facilitate the process of seeking verifiable parental consent is appropriate given the increased utilization of text messaging and mobile phones in the United States.[52] Commenters also suggested that mobile communication mechanisms are more likely than some other approved consent methods to result in operators reaching parents for the desired purpose of providing

[49] 89 FR 2034 at 2040.
[50] In the 2024 NPRM, the Commission explained the basis for its conclusion that increased use of "over-the-top" messaging platforms, which are platforms that utilize the Internet instead of a carrier's mobile network to exchange messages, means that mobile telephone numbers now permit direct contact with a person online and therefore can be treated as online contact information consistently with the COPPA statute. *See* 89 FR 2034 at 2041.
[51] *See, e.g.*, Future of Privacy Forum, at 2-3; Computer and Communications Industry Association ("CCIA"), at 2-3; Association of National Advertisers ("ANA"), at 15-16; The Toy Association, at 2; Chamber, at 4; EPIC, at 4; kidSAFE, at 2; Epic Games, Inc. ("Epic Games"), at 4-5; Consumer Technology Association, at 2-3; Consumer Reports, at 3; Children and Screens, at 3; M. Bleyleben, at 1-2; TechNet, at 3; Software and Information Industry Association ("SIIA"), at 3. *See also, e.g.*, ITIC, at 2 (supporting permitting operators to send text messages to parents for the purposes of initiating verifiable parental consent); Advanced Education Research and Development Fund, at 8 (same); BBB National Programs/Children's Advertising Review Unit ("CARU"), at 2-3 (asserting that the benefits of operators contacting parents via text messages likely outweigh the security risks).
[52] *See, e.g.*, CCIA, at 2-3; ANA, at 16; Epic Games, at 4; SIIA, at 3; Consumer Reports, at 3.

notice and obtaining consent, and that sending a text message may be one of the most direct and frictionless methods of contacting a parent.[53]

While not clearly opposing the proposal, one FTC-approved COPPA Safe Harbor program, Privacy Vaults Online, Inc. ("PRIVO"), suggested that the use of text messages to seek parental consent might make it more difficult for parents to recognize senders, review disclosures, and contact the operator if they subsequently decide to withdraw consent.[54] In response, the Commission notes that these issues can also be challenges associated with other methods of communication, such as email. PRIVO further suggested children's provision of parents' mobile telephone numbers may expose parents to increased data mining and profiling because, while many adults have multiple email accounts, they frequently have only one mobile telephone number, thereby enabling use of the number to profile an individual.[55] In response, the Commission notes that § 312.5(c)(1) restricts the purpose for which online contact information can be collected under that exception to providing notice and obtaining parental consent.[56] Although mindful of the concerns raised by commenters, the Commission finds that parents' mobile telephone numbers are likely an effective way to reach parents and believes these concerns are outweighed by the strong interest in facilitating effective communication between operators and parents to initiate the process of seeking and obtaining consent.

---

[53] *See, e.g.*, kidSAFE, at 2 (suggesting proposed change "will greatly alleviate the burden of operators initiating a parental consent flow … and increase the chances of the parent actually receiving and completing the consent request"); CARU, at 2-3 (permitting use of text messages to initiate verifiable parental consent may improve ease and accessibility); CCIA, at 3 (suggesting text messages are "one of the most direct and frictionless verifiable methods for contacting a parent to provide notice or obtain consent"); Epic Games, at 4 (asserting proposal will enhance operators' ability to connect with parents and "text messaging appears to be a common and trusted platform among consumers"); M. Bleyleben, at 1-2 ("Allowing operators to communicate with parents via mobile messaging will broaden access and reduce friction for parents to provide parental consent (thereby also reducing incentives for children to circumvent the age gate).").

[54] Privacy Vaults Online, Inc. ("PRIVO"), at 3-4.

[55] *Id.* at 2-3. PRIVO did not provide specific evidence to assess these potential impacts.

[56] 16 CFR 312.5(c)(1) ("Where the *sole* purpose of collecting the name or online contact information of the parent or child is to provide notice and obtain parental consent under § 312.4(c)(1).") (emphasis added).

A minority of commenters opposed the proposal to amend the definition of "online contact information."[57] Commenters opposing the proposed amendment generally cited possible security risks for recipients of text messages related to malicious links and phishing.[58] However, more commenters addressing this issue suggested that the use of email messages to initiate the verifiable parental consent process poses comparable security risks.[59] A number of commenters suggested that operators could take steps to reduce such security risks.[60] Based on the record, the Commission believes that the security risks associated with initiating the process of seeking verifiable parental consent via text message are comparable to the risks associated with initiating the verifiable parental consent process via other communication methods, such as email. The Commission expects that operators will take steps to reduce security risks to recipients of text messages.

Some commenters suggested that sending text messages to mobile telephone numbers without the consent of mobile telephone subscribers might have the potential to conflict with

[57] Internet Safety Labs, at 3; Parent Coalition for Student Privacy, at 11. Commenters also addressed potential security risks in response to Question Three in the "Questions for the Proposed Revisions to the Rule" section of the 2024 NPRM. *See* 89 FR 2034 at 2069 (Question 3).

[58] *See, e.g.*, Parent Coalition for Student Privacy, at 11; Internet Safety Labs, at 3 (suggesting proposed change would facilitate phishing). Other commenters that supported, or did not explicitly oppose, the addition of mobile telephone numbers as a category of online contact information in order to permit operators to use text messages to initiate verifiable parental consent noted some of the same potential security risks. *See, e.g.*, City of New York Office of Technology and Innovation ("NYC Technology and Innovation Office"), at 3 (citing increased risk of malicious text messages or "smishing"); B. Hills, at 5 (expressing concern about increased risk of scams with malicious verification links).

[59] *See, e.g.*, Consumer Reports, at 3 (suggesting risks associated with the use of text messages are not appreciably stronger than the risks with existing contact methods such as email); Future of Privacy Forum, at 2 (suggesting risks associated with the use of text messages are no greater than with the use of existing contact methods such as email); Epic Games, at 4 (suggesting security risks associated with use of text messages are relatively low and not higher or worse than those associated with the use of email); M. Bleyleben, at 2 (same). One of these commenters suggested that security risks can be mitigated because parents can check with their children to determine if they initiated the process before proceeding. *See* Future of Privacy Forum, at 2.

[60] *See* SIIA, at 14 (suggesting security risk is minimal and can be ameliorated); Heritage Foundation, at 1 (suggesting risks of undetected spam from text may be higher than email, but platforms could employ methods that avoid risks associated with recipients clicking on links). *See also* kidSAFE, at 2 (asserting that, if the Commission approved the use of text messages to obtain verifiable parental consent, the inputting of a code received in a text message could mitigate risks associated with clicking on malicious links in text messages).

federal and state laws related to text messaging[61] and warned that operators might rely on a Commission rule (the potentially amended COPPA Rule) permitting the collection of mobile telephone numbers without a full appreciation of other regulatory requirements related to sending text messages.[62] While not opposing the proposal, one such commenter contended that the Telephone Consumer Protection Act, the National Do-Not-Call Registry, and an Oklahoma statute "all require prior express consent of the recipient to receive various types of text messages, including marketing messages."[63] The commenter further indicated there is some uncertainty about what constitutes a commercial or marketing message under existing laws, and that it is not clear that children can legally consent on behalf of a parent to the transmission of a text message to a parent's mobile phone number.[64] The Commission agrees that it is important for operators and others to carefully consider, and comply with, all applicable state and federal laws when making decisions about whether and how to collect and use mobile telephone numbers.[65] The analysis of relevant factual considerations and laws that commenters provided on this issue was limited, but the Commission believes these comments potentially overstate the degree of conflict and expects the content of text messages as well as other decisions related to implementation likely would be important in complying with legal obligations.

At least one commenter expressed confusion about whether the Commission intended the proposed Rule amendments to constitute approval of operators' use of text messages to obtain

[61] Chamber, at 4 (asking Commission to verify that collection and use of mobile phone number provided by children to contact parents to start notice and consent process will not violate relevant federal or state laws); The Toy Association, at 2 (alluding to possible conflict between proposed collection and use of mobile phone numbers under the Rule and the Telephone Consumer Protection Act and related state laws).
[62] PRIVO, at 4.
[63] *Id.* at 2. *See also* The Toy Association, at 2.
[64] PRIVO, at 2. PRIVO also suggested parents will not recognize numbers associated with such text messages, which could lead parents to decide not to provide consent or might make it difficult for parents to know how to change their consent decision or request review of their children's data later. *Id.* at 3.
[65] The Commission notes that many states have enacted laws regulating commercial text messages. *See, e.g.*, Conn. Gen. Stat. § 42-288a; Fla. Stat. § 501.059; Wash. Rev. Code § 19.190.060 et seq.

verifiable parental consent.[66] Other commenters encouraged the Commission to approve text messaging as a mechanism for obtaining verifiable parental consent.[67] In response, the Commission clarifies that it is amending the definition of "online contact information" and has decided to make a related amendment to § 312.5(b)(2) of the Rule discussed in Part II.D.7. That amendment to § 312.5(b)(2) will permit operators to send text messages to parents to initiate the process of seeking verifiable parental consent, provide direct notice to the parent, and obtain verifiable parental consent, in situations where a child's personal information is not being disclosed, consistent with a new "text plus" verifiable parental consent method the Commission is approving and adding as § 312.5(b)(2)(ix).

The Commission is also adjusting the definition of "online contact information" proposed in the 2024 NPRM to limit the use of mobile telephone numbers, in the absence of verifiable parental consent, to purposes related to obtaining verifiable parental consent. In the 2024 NPRM, the Commission discussed the importance of avoiding situations where mobile telephone numbers collected from children would be used to make voice calls to children without parental consent. After carefully considering the record and comments, the Commission has adjusted the proposed language to prevent situations where operators are utilizing mobile telephone numbers collected from a child for purposes unrelated to obtaining verifiable parental consent.[68]

---

[66] *See* Entertainment Software Rating Board ("ESRB"), at 22-23.

[67] *See, e.g.*, Program on Economics & Privacy at Scalia Law School and Brechner Center for the Advancement of the First Amendment at University of Florida ("Scalia Law School Program on Economics & Privacy and University of Florida Brechner Center"), at 2; TechNet, at 3-4; Consumer Technology Association, at 3; Privacy for America, at 10-11; ANA, at 15-16; ACT | The App Association, at 7.

[68] At least one commenter requested clarification as to whether the amendment to the "online contact information" definition proposed in the 2024 NPRM was intended to allow operators to use mobile telephone numbers for other purposes set forth in § 312.5(c) of the Rule. kidSAFE, at 2. The Commission did not intend such a result and is therefore modifying the proposed amendment to the definition. For example, the Commission wants to avoid situations where operators use mobile telephone numbers to contact a child multiple times through either text messages or voice calls without verifiable parental consent.

c. The Commission Adopts Amendments Regarding "Online Contact Information"

After carefully considering the record and comments, and for the reasons discussed in Part II.B.2.b of this document, the Commission has decided to adopt an amended version of the proposed addition to the definition of "online contact information" to include "or a mobile telephone number provided the operator uses it only to send text messages to a parent in connection with obtaining parental consent."

3. Definition of "Personal Information"

The COPPA statute and the COPPA Rule define "personal information" as individually identifiable information about an individual collected online, including, for example, a first and last name, an e-mail address, or a Social Security number. The COPPA statute also authorizes the Commission to include within the COPPA Rule's definition of personal information "any other identifier that the Commission determines permits the physical or online contacting of a specific individual."[69] Accordingly, as discussed in Part II.3.a and b, the Commission has decided to include biometric identifiers in the definition of "personal information. However, in response to comments, the Commission is adopting a modified version of the definition proposed in the 2024 NPRM.

a. The Commission's Proposal Regarding "Personal Information"

In the 2024 NPRM, the Commission proposed using its statutory authority to expand the Rule's coverage by amending the 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

[69] 15 U.S.C. 6501(8)(F).

sequence; or data derived from voice data, gait data, or facial data."[70] The Commission explained this proposed amendment is intended to ensure that the Rule is keeping pace with technological developments that facilitate increasingly sophisticated means of identifying individuals.[71] The Commission has determined that biometric recognition technologies have rapidly advanced since the 2013 Amendments to the Rule,[72] and biometric identifiers such as fingerprints, handprints, retina and iris patterns, and DNA sequences can be used to identify and contact a specific individual either physically or online.[73]

b. Public Comments Received in Response to the Commission's Proposal Regarding "Personal Information"

[70] *See* 89 FR 2034 at 2041.
[71] *Id*.
[72] *Id*. For example, the National Institute of Standards and Technology ("NIST") found that, between 2014 and 2018, facial recognition became 20 times better at finding a matching photograph from a database. *See* NIST, *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification* (2018), at 6, available at *https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf*. *See also* U.S. Government Accountability Office, *Biometric Identification Technologies: Considerations to Address Information Gaps and Other Stakeholder Concerns* (Apr. 2024), at 1, available at *https://www.gao.gov/assets/gao-24-106293.pdf* (observing that use of facial and iris recognition technologies to conduct and automate identification has become "increasingly common in both the public and private sectors"); NIST, Press Release, *NIST Evaluation Shows Advance in Face Recognition Software's Capabilities* (Nov. 30, 2018), available at *https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwarescapabilities*.
[73] *See* U.S. Government Accountability Office, *Facial Recognition Technology: Current and Planned Uses by Federal Agencies* (Aug. 2021), at 3, available at *https://www.gao.gov/assets/gao-21-526.pdf* (citing biometric technologies used to identify individuals by measuring and analyzing physical and behavioral characteristics, including faces, fingerprints, eye irises, voice, and gait). The Commission notes that law enforcement authorities and agencies are using a variety of biometric-based technologies to identify and contact individuals. For example, the FBI has stated that its Next Generation Identification utilizes fingerprints, palm prints, and facial recognition to identify individuals of interest in criminal investigations, and that it is developing a repository of iris images. *See* FBI Law Enforcement Resources, available at *https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/biometrics/next-generation-identification-ngi*. *See also* U.S. Government Accountability Office, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks* (June 2021) (surveying use of facial recognition technology by twenty federal agencies). The FBI reported that its Combined DNA Index Systems included 20 million DNA profiles in 2021, and it is used to link crime scene evidence to other cases or to persons already convicted of or arrested for specific crimes. *See* FBI National Press Office, *The FBI's Combined DNA Index System (CODIS) Hits Major Milestone* (May 21, 2021), available at *https://www.fbi.gov/news/press-releases/the-fbis-combined-dna-index-system-codis-hits-major-milestone#:~:text=May%2021,%202021.%20The%20FBI%E2%80%99s%20Combined%20DNA%20Index%20System%20(CODIS)*.

Many commenters expressed general support for amending the Rule's definition of personal information to include biometric identifiers.[74] Supportive commenters emphasized the uniquely personal nature of biometric identifiers and noted that there are particularly compelling privacy interests in protecting such sensitive data.[75] Moreover, unlike certain other identifiers, such as email addresses, telephone numbers, or first and last names, biometric identifiers are generally immutable.[76] Commenters also expressed concern about the fact that the expanded collection of biometric data from children online[77] and from wearable devices with sensor technology[78] increases the risk of abuse and sale of such data. Commenters discussed the potential for biometric data to be combined with other persistent identifiers such as IP addresses or device IDs to identify specific individuals[79] and also cited concerns about tools utilizing

[74] *See, e.g.*, B. Hills, at 4; Common Sense Media, at 13; S. Winkler, at 1; Children and Screens, at 5; NYC Technology and Innovation Office, at 1-2; Lawyers' Committee for Civil Rights Under Law ("Lawyers' Committee"), at 6; EPIC, at 4; Internet Safety Labs, at 4; Mental Health America, at 4-5; American Civil Liberties Union ("ACLU"), at 13; Center for AI and Digital Policy, at 5; IEEE Consortium for Innovation and Collaboration in Learning Engineering ("IEEE Learning Engineering Consortium"), at 5; Parent Coalition for Student Privacy, at 12; PRIVO, at 4; Attorneys General of Oregon, Illinois, Mississippi, Tennessee, Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Indiana, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, South Dakota, Utah, Vermont, Virgin Islands, Virginia, Washington, and Wisconsin ("State Attorneys General Coalition"), at 2-3; Consortium for School Networking, at 3; Center for Democracy and Technology ("CDT"), at 5; Google, at 3; Consumer Reports, at 4; Center for Digital Democracy, Fairplay, American Academy of Pediatrics, Berkeley Media Studies Group, Children and Screens: Institute of Digital Media and Child Development, Consumer Federation of America, Center for Humane Technology, Eating Disorders Coalition for Research, Policy, & Action, Issue One, Parents Television and Media Council, and U.S. PIRG ("Children's Advocates Coalition"), at 58; Data Quality Campaign, at 3.

[75] *See, e.g.*, Children and Screens, at 5; NYC Technology and Innovation Office, at 1-2; Lawyers' Committee, at 6; Consortium for School Networking, at 3; Consumer Reports, at 4-5; ACLU, at 13; Data Quality Campaign, at 3.

[76] *See, e.g.*, Mental Health America, at 4 ("Biometric identifiers are generally immutable and could potentially be used to identify a child for the rest of their life."); NYC Technology and Innovation Office, at 1 ("A person cannot easily alter, if at all, their fingerprints, ocular scans, facial features, or genetic data. This makes biometric information particularly sensitive…[.]"); ACLU, at 13 (noting that "biometrics are inherently personally identifying and generally immutable"); Data Quality Campaign, at 3 ("The immutable nature of biometrics means improper access or use can permanently expose children to unwanted risks.").

[77] *See, e.g.*, State Attorneys General Coalition, at 3; Children's Advocates Coalition, at 58-60.

[78] *See, e.g.*, State Attorneys General Coalition, at 3 (discussing increased use of wearable devices with sensors and noting that "[t]he prevalence of the collection and use of this type of data – from using a fingerprint to unlock a device to wearable sensors – has resulted in a heightened risk of abuse and sale of this type of data, data that is often immutable and permanently tied to the individual"); Children's Advocates Coalition, at 59 (discussing collection of biometric data by large platforms and virtual reality products and services).

[79] *See* State Attorneys General Coalition, at 3.

machine learning or artificial intelligence being used to duplicate and misuse such data.[80] A children's advocates coalition expressed concern about the "unreasonable unnecessary collection of biometric information for mass profiling, neuromarketing, targeted advertising, advanced behavioral analytics, behavioral advertising … product improvement, and engagement maximization."[81] Commenters also highlighted harms related to the misuse of biometric data to impersonate individuals through deepfake technologies,[82] and the particularly grave harms associated with child sexual abuse material generated using such biometric data.[83] The Commission finds these concerns compelling. A principal benefit to including biometric identifiers in the definition of personal information is to protect children under 13 from the misuse of this immutable and particularly sensitive information, which can potentially be used to identify a child for the rest of their life. While it is impossible to quantify, the Commission considers protecting children under 13 from the potential misuse of this highly sensitive information to be a significant benefit of the proposed amendment.

A number of commenters that generally supported adding in the definition of personal information a new provision for biometric data encouraged the Commission to consider expanding the biometric identifier provision in the definition of personal information beyond

[80] *See, e.g.*, Center for AI and Digital Policy, at 4-5; S. Winkler, at 1. *See also Comment of the Federal Trade Commission In the matter of: Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts*, Fed. Commc'ns Comm'n CG Docket No. 23-362 (July 29, 2024) (describing some of the FTC's efforts to address the emergence of new technologies powered by artificial intelligence, particularly those related to voice cloning), available at *https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-Comment-VoiceCloning.pdf.*

[81] *See* Children's Advocates Coalition, at 60.

[82] *See, e.g.*, Center for AI and Digital Policy, at 5; S. Winkler, at 1. *See also* DHS Public-Private Analytic Exchange Program, *Increasing Threats of Deepfake Identities*, at 9-18, 22-25 (discussing how deepfakes using biometric data are made and their use in non-consensual pornography and cyberbullying), available at *https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf.*

[83] *See* Center for AI and Digital Policy, at 5.

what the Commission proposed in the 2024 NPRM.[84] For example, one commenter encouraged the Commission to consider adding more examples of biometric identifiers such as electroencephalogram patterns used in brain-computer interfaces, heart rate patterns, or behavioral biometrics such as typing patterns or mouse movements.[85] Some consumer groups suggested the Commission should expand the provision to include any information derived from biometric data.[86] Another suggestion was that the Commission broaden the provision to make it consistent with the Commission's definition of the term "biometric information" in a recent Commission policy statement.[87] A coalition of state attorneys general urged the Commission to consider language that would include "imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings (from which an identifier template such as a faceprint, a minutiae template, or a voiceprint, can be extracted), genetic data, or other unique biological, physical, or behavioral patterns or characteristics, including data generated by any of these data points."[88]

[84] In Question Five in the "Questions for the Proposed Revisions to the Rule" section of the 2024 NPRM, the Commission asked commenters to address whether it should consider including any additional biometric identifier examples beyond those listed in the proposed definition. 89 FR 2034 at 2070 (Question 5).
[85] IEEE Learning Engineering Consortium, at 5. *See also* Parent Coalition for Student Privacy, at 12 (recommending expanding the proposed list of biometric identifiers to include keystroke dynamics); B. Hills, at 4 (recommending adding vein recognition); Internet Safety Labs, at 4 (recommending adding typing cadence); State Attorneys General Coalition, at 2-3. Some commenters proposed adding sensitive categories of information such as student behavioral data, health data, and geolocation data to the definition of personal information. *See, e.g.*, K. Blankinship, at 1; State Attorneys General Coalition, at 3. The Commission notes that at least some forms of student behavioral data and health data currently receive protection under the United States Department of Education's Family Educational Rights and Privacy Act Regulations, 34 CFR Part 99, and the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191. Moreover, the definition of personal information already includes geolocation data that is sufficient to identify street name and name of a city or town, which is the geolocation data that is most likely to permit identifying and contacting a specific child. *See* 78 FR 3972 at 3982-3983 (discussing personal information definition's coverage of geolocation data).
[86] *See, e.g.*, Children's Advocates Coalition, at 58; Mental Health America, at 4.
[87] Center for AI and Digital Policy, at 5 (discussing Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act).
[88] State Attorneys General Coalition, at 2.

For a variety of reasons, a significant number of industry group and other commenters opposed the biometric identifier provision proposed in the 2024 NPRM.[89] Commenters argued the proposal exceeds the Commission's statutory authority because the Commission has not established that the biometric identifiers enumerated in the 2024 NPRM proposal enable the physical or online contacting of a specific child.[90] The Commission disagrees. As explained in this Part, 15 U.S.C. 6501(8)(F) provides that "[t]he term 'personal information' means individually identifiable information about an individual collected online, including…any…identifier that the Commission determines permits the physical or online contacting of a specific individual," and for several reasons, the Commission has determined that biometric information permits the physical or online contacting of a specific individual.

The Commission notes that the proposed expansion of the definition of personal information to include biometric identifiers appropriately responds to marketplace developments such as the increasingly common use of technologies relying on facial recognition, retina or iris imagery, or fingerprints to allow individuals to unlock mobile devices and to access accounts or facilities,[91] and that enable companies to identify and contact a specific individual. Genetic data,

[89] *See, e.g.*, R Street Institute, at 1-2; ITIC, at 2; CIPL, at 4-5; ESA, at 9-11; SIIA, at 4, 15; ACT | The App Association, at 4-5; Chamber, at 3; IAB, at 2-5; NCTA, at 5-6; NetChoice, at 3-4; Information Technology and Innovation Foundation ("ITIF"), at 3; CCIA, at 3-4; ANA, at 10; Privacy for America, at 14-15; Epic Games, at 7-8.
[90] *See, e.g.*, ESA, at 9-11; NCTA, at 5; CCIA, at 3. *See also* NetChoice, at 3-4 (suggesting the Commission has not demonstrated that biometric data is being misused in ways that allow contact with children).
[91] *See* ACT | The App Association, at 4 (noting that many new apps collect biomarkers such as voice, facial features, and fingerprints in some form). *See also* R. L. German & K. S. Barber, *Current Biometric Adoption and Trends* (November 2016), at 2-13 (analyzing adoption of biometric authentication between 2004 and 2016 and concluding that rapid expansion of biometric technologies has led to similar explosion in biometric services and applications), available at *https://identity.utexas.edu/sites/default/files/2020-09/Current%20Biometric%20Adoption%20and%20Trends.pdf*; H. Kelly, *Fingerprints and Face Scans Are the Future of Smartphones. These Holdouts Refuse to Use Them*, Washington Post (Nov. 15, 2019), available at *https://www.washingtonpost.com/technology/2019/11/15/fingerprints-face-scans-are-future-smartphones-these-holdouts-refuse-use-them/*; National Retail Federation, *2023 National Retail Survey* (Sept. 26, 2023), at 18 (stating that 40% of retail survey respondents were researching, piloting, or implementing either facial recognition or feature-matching technologies to address loss prevention and other security concerns), available at *https://nrf.com/research/national-retail-security-survey-2023*.

particularly when combined with other personal information, can also be used to identify and, in some circumstances, contact a specific individual.[92] Gait[93] and other movement patterns[94] can also be used to identify and contact specific individuals and are an increasing concern with the growth of virtual reality products and services. The Commission also expects that biometric identifiers, particularly when combined with increasingly sophisticated methods of consumer profiling, potentially could be used to track and deliver targeted advertisements to specific children online, which would constitute online contact.[95] Accordingly, biometric identifiers are appropriately included in the definition of "personal information."

Other commenters objecting to the proposed biometric identifier provision argued that it is inconsistent with the COPPA statute because the enumerated biometric identifiers do not necessarily identify a specific individual.[96] In response, the Commission notes that the Rule's definition of personal information is consistent with the COPPA statute because it remains expressly limited to "individually identifiable information about an individual," and the proposed

---

[92] *See, e.g.*, S. Y. Rojahn, *Study Highlights the Risk of Handing Over Your Genome: Researchers found they could tie people's identities to supposedly anonymous genetic data by cross referencing it with information available online*, MIT Technology Review (Jan. 17, 2013), available at *https://www.technologyreview.com/2013/01/17/180448/study-highlights-the-risk-of-handing-over-your-genome/*; Natalie Ram, *America's Hidden National DNA Database*, 100 Texas Law Review, Issue 7 (July 2022) (discussing growth of investigative genetic genealogy searches using private platforms and surveying state law policies related to potential law enforcement access to newborn genetic screening samples), available at *https://texaslawreview.org/americas-hidden-national-dna-database/*.

[93] L. Topham et al., *Gait Identification Using Limb Joint Movement and Deep Machine Learning*, IEEE Access (Sept. 19, 2022), available at *https://ieeexplore.ieee.org/document/9895247*; D. Kang, *Chinese 'gait recognition' tech IDs people by how they walk*, Associated Press (Nov. 6, 2018), available at *https://apnews.com/article/bf75dd1c26c947b7826d270a16e2658a*.

[94] *See* V. Nair et al., *Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data* (Feb. 17, 2023), at 1 (reporting results showing virtual reality users can be uniquely and reliably identified out of a pool of over 50,000 candidates with 94.33% accuracy based on 100 seconds of head and hand motion data), available at *https://arxiv.org/pdf/2302.08927*.

[95] The plain meaning of "contact" is broader than just an email or other communication, and the legislative history of the COPPA statute also supports a broad interpretation of the term. At the time of adoption, Senator Bryan noted that the term "is not limited to e-mail, but also includes any other attempts to communicate directly with a specific, identifiable individual." *See* 144 Cong. Rec. S12741-04, S12787 (1998) (statement of Senator Bryan).

[96] *See, e.g.*, ITIF, at 3. Some generally supportive commenters also emphasized the importance of ensuring that the definition only includes biometric identifiers that can be used to identify and contact a specific child. *See, e.g.*, Common Sense Media, at 13; The Toy Association, at 3.

provision for "biometric identifier" only includes "a biometric identifier that can be used for the automated or semi-automated recognition of an individual." Further, the Commission finds that the biometric identifiers listed as examples in the proposed definition can be used to identify specific individuals.[97]

Commenters also encouraged the Commission to consider the costs and benefits of constraining the collection and use of biometric identifiers,[98] including considering the impact the proposed biometric identifier provision would have on innovation and on beneficial uses such as security and authentication features.[99] In response, the Commission notes that the commenters raising these and similar concerns did not provide information or evidence quantifying the potential costs and impacts associated with adding the new biometric identifier provision to the personal information definition. The amendment does not impact the collection or use of biometric identifiers from users over the age of 12. Because the proposed biometric identifier provision only requires that covered operators provide appropriate notice and obtain verifiable parental consent before collecting, using, or disclosing this sensitive data from children, it is not clear that the proposed provision would significantly interfere with innovation or beneficial uses of biometric identifiers. However, in consideration of these and other

[97] For example, a recent GAO Report found that "a wide range of technologies [] can be used to verify a person's identity by measuring and analyzing biological and behavioral characteristics" and specifically mentioned facial data, fingerprints, iris, voice, hand geometry, and gait. *See* U.S. Government Accountability Office, *Biometric Identification Technologies: Considerations to Address Information Gaps and Other Stakeholder Concerns* (April 2024), at 4-5, available at *https://www.gao.gov/assets/gao-24-106293.pdf*. *See also* A. K. Jain et al., *50 years of biometric research: Accomplishments, challenges, and opportunities,* Pattern Recognition Letters, Volume 79 (Aug. 2016), at 80-83, available at *https://www.sciencedirect.com/science/article/abs/pii/S0167865515004365*.

[98] *See, e.g.*, ITIC, at 2 (suggesting expansion of personal information to include biometric data requires a detailed assessment of costs and benefits, including impacts on innovation and that additional work is required to ensure that any inclusion of biometric data is narrowly tailored to clear, evidenced harms); IEEE Learning Engineering Consortium, at 5 (recommending that the Commission periodically review the list of biometric identifiers in the definition to make sure it remains comprehensive and relevant and consider the context in which biometric identifiers are being collected and used).

[99] *See, e.g.*, kidSAFE, at 4 (discussing use of biometric data for security purposes); ACT | The App Association, at 4 (expressing general concern about the provision's impact on innovation); ITIF, at 2 (same).

comments, the Commission has decided to adopt a modified version of the biometric identifier provision proposed in the 2024 NPRM.

Some commenters urged the Commission to consider adjusting the language proposed in the 2024 NPRM to reduce perceived inconsistencies between the proposed biometric identifier provision and various state laws and industry standards.[100] For example, one industry commenter indicated the term "biometric identifier" is not commonly used in other laws and regulations and recommended instead using the term "biometric data" to align with other laws and industry standards to reduce confusion and help operators fulfill their compliance obligations.[101] Another commenter suggested the proposed provision is inconsistent with state laws related to biometric information that exclude audio recordings, videos, and photos from their definitions.[102] In response, the Commission notes that the COPPA Rule applies to personal

[100] *See, e.g.*, M. Bleyleben, at 2 (suggesting that it is critical that the Commission's approach to defining and scoping the use of biometric technologies is coordinated with state-level biometric laws such as the Biometric Information Privacy Act in Illinois); CIPL, at 4-5 (suggesting the term biometric identifier is not aligned with the International Organization for Standardization and other laws and regulations); ESA, at 10-11 (discussing state laws that exclude audio recordings, videos, and photos from definitions of biometric information); SIIA, at 4 (opposing biometric identifier provision and suggesting it creates inconsistencies with state privacy laws); IAB, at 3-4 (discussing differences between proposed biometric identifier provision and biometric definitions in various state privacy laws); Chamber, at 3 (encouraging the Commission to harmonize proposed biometric identifier provision with other laws modeled on Consensus State Privacy Approach, and citing the definition of biometric data in the Virginia Consumer Data Protection Act); NCTA, at 6 (arguing Commission's proposal conflicts with state biometric laws, which consider derived data to be biometric data only where it is used or intended to be used to identify a specific individual); ITIF, at 3 (stating that many states have enacted privacy legislation to protect biometric data and have limited their definitions to biometric data that identifies a specific individual). On the other hand, at least one supportive commenter suggested the proposed biometric identifier provision would better align the Rule's personal information definition with FERPA. *See* Data Quality Campaign, at 3.

[101] CIPL, at 4. In response, the Commission notes that it is using the term biometric identifier rather than the term biometric data to align with the definition of personal information in the COPPA statute. There is some variation in the defined terms different state privacy and biometric laws use, but Texas, Illinois, and Washington state laws use the term biometric identifier. The Illinois Biometric Information Privacy Act defines that term to mean "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" and excludes a variety of other types of information such as written signatures, photographs, or human biological samples used for scientific testing or screening. *See* 740 Ill. Comp. Stat. 14/10. Washington's biometric privacy law defines that term to mean "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." Wash. Rev. Code 19.375.010.

[102] *See, e.g.*, ESA, at 10-11; IAB, at 3-4. It is not clear why the proposed new provision for biometric identifiers generates concerns for industry commenters about inconsistencies related to the treatment of photographs, videos, or

information collected from children online by operators of child-directed websites and online services and operators of general audience websites or online services that have actual knowledge they are collecting personal information from children. State laws' approaches to biometric data may be different, in part, because of the different obligations those laws impose on businesses or because those laws apply to data collected from a large population of users.[103]

Other commenters urged the Commission to consider limiting the proposed biometric identifier provision to biometric identifiers that are used or intended to be used to recognize or identify an individual, to better align with state laws and to simplify operators' compliance obligations.[104] While recognizing there is some variability in defined terms among state privacy laws and also between those laws and the biometric identifier provision in the proposed definition of personal information, industry commenters raising these concerns have not explained how those variations will complicate business practices or create irreconcilable compliance obligations.[105] The Commission is therefore not persuaded that the proposed amended definition of personal information should be changed to align with specific state laws, particularly when there is variation among such laws.

---

audio files under state law when paragraph 8 of the COPPA Rule's personal information definition currently has a separate provision for such data when they contain a child's image or voice. *See* 16 CFR 312.2.

[103] The Commission also notes that use of the term biometric identifier comports with language in the definition of personal information in the COPPA statute. *See* 15 U.S.C. 6501(8)(F).

[104] *See, e.g.*, Privacy for America, at 15 (citing Connecticut statute's definition of biometric data as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual"); NCTA, at 6 (suggesting the NPRM proposal conflicts with state biometric laws, which consider derived data to be biometric data only where it is used or intended to be used to identify a specific individual); ANA, at 10 (suggesting biometric identifier provision should be limited to instances where biometric information is used or intended to be used to recognize or identify a child rather than data that can theoretically be used for that purpose but is not used in that way and further arguing this approach better aligns with the definitions of similar terms in the majority of state privacy laws and regulations) (citing Cal. Civ. Code 1798.140(c); 4 CCR 904-3, Rule 2.02; Va. Code Ann. 59.1-575); CIPL, at 4-5.

[105] *See, e.g.*, ITIF, at 3 (contending that a materially different definition of biometric identifiers in the COPPA Rule would complicate an already complex regulatory environment in the United States and would create consumer confusion, increase compliance costs on businesses and adversely impact the digital economy); Chamber, at 3.

Other commenters suggested the proposed biometric identifier provision should be similarly narrowed for different reasons. For example, several industry commenters suggested adjusting the provision from biometric identifiers that "can be used" for automated or semi-automated recognition to a biometric identifier that "is used" for automated recognition of an individual, to, in their view, be more consistent with the definition of personal information in the COPPA statute and to avoid vagueness concerns.[106] Other commenters suggested the provision should only include biometric identifiers that are intended to be used for identification, or suggested that there should be an exception when biometric identifiers are used to provide a service without identifying the user.[107] Still others urged the Commission to narrow the biometric identifier provision to a specific list of biometric identifiers and to limit coverage to situations where the biometric identifier is used to contact a child.[108]

In response, the Commission notes that it disagrees with these commenters' assertions that such adjustments are necessary to comport with the COPPA statute. The phrase "can be used" is consistent with the COPPA statute, which defines personal information to mean "individually identifiable information about an individual collected online" rather than an alternative such as information used to identify an individual.[109] Further, the Commission believes the proposed language is consistent with the statutory language in 15 U.S.C. 6501(8)(F), which permits the addition of "any other identifier the Commission determines permits the

[106] *See, e.g.*, Chamber, at 3 (arguing that the Commission should revise the definition to include biometric identifiers only when they are used for the automated recognition of an individual rather when they could be used for such purposes to avoid vagueness concerns); ACT | The App Association, at 4-5 (suggesting definition must be limited to when a biometric identifier is used to identify or reasonably identify a child to comport with the COPPA statute); Privacy for America, at 15 (contending the provision should be limited to biometric identifiers used to identify a child in order to contact them); The Toy Association, at 3 (contending an actual use element needs to be included in the definition to comport with the COPPA statute). *See also* CIPL, at 4-5.
[107] *See, e.g.*, CIPL, at 5 (suggesting there should be an intent component included in the provision); ITIC, at 2 (contending that the Commission should clarify that any use of biometric data that does not involve identifying a unique individual and that does not allow physical or online contact with a specific individual is exempt).
[108] *See* NCTA, at 6.
[109] 15 U.S.C. 6501(8).

physical or online contacting of a specific individual" rather than alternative language such as "identifiers when used to contact a specific individual physically or online." Additionally, the other identifiers listed in the definition in the COPPA statute qualify as personal information regardless of how an operator uses them. The Commission also believes that adjusting the proposed language from "can be used for the automated or semi-automated recognition of an individual" to language requiring actual use of biometric identifiers to identify individuals may increase opportunities for operators to collect and retain sensitive data for future use and would also present enforcement challenges.

Numerous commenters were particularly critical of the Commission's proposal to include the words "data derived from voice data, gait data, or facial data" in the biometric identifier provision the Commission proposed in the 2024 NPRM.[110] Many commenters suggested this language is overbroad or vague.[111] Some commenters also argued such data is not necessarily individually identifying and cannot be used to contact a specific child, and therefore falls outside the scope of personal information protected by the COPPA statute.[112] Commenters contended this aspect of the biometric provision may stifle innovation[113] and interfere with uses of biometric information such as virtual reality applications, educational technology products,

[110] *See, e.g.*, ANA, at 10; Chamber, at 3; kidSAFE, at 3-4; Epic Games, at 7-8; NCTA, at 5-6.
[111] *See, e.g.*, CARU, at 3 (suggesting unclear whether data from an avatar based on the user or data from an accelerometer in a connected toy would be included in data derived from voice data, gait data, or facial data); kidSAFE, at 3-4 (suggesting breadth of proposed language may cover unintended data and requesting that the Commission provide clarifying examples and indicate whether it intends to include data tracking the motion of a child in a virtual reality game, analysis of a child's ability to pronounce certain words or sounds, or the text transcript of a child's audio conversation with a connected toy device); ESA, at 10; Chamber, at 10; ANA, at 10. Others suggested that including data derived from voice data in the proposed definition of personal information is potentially inconsistent with the approach adopted in the Commission's Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings. *See, e.g.*, ESA, at 10.
[112] *See, e.g.*, ESA, at 9-10; Epic Games, at 7-8.
[113] *See, e.g.*, CARU, at 3.

connected toys, or speech-enabled apps used by children or individuals with disabilities.[114] Others suggested that treating such derived data as personal information would constrain desirable use cases such as security features.[115] Still other commenters opposing the proposal argued that it conflicts with relevant state laws and the 2024 NPRM's proposal to except from the COPPA Rule's verifiable parental consent requirement operators' collection of certain audio files that contain a child's voice.[116] To reduce the potential burdens and impacts these and other commenters mentioned, the Commission has decided not to include this language in the biometric identifier provision as proposed in the 2024 NPRM.

After carefully considering the record and comments, the Commission has decided to adopt an amended version of the biometric identifier provision the Commission proposed in the 2024 NPRM. The Commission previously explained that the proposed provision included a non-exhaustive list of examples of covered biometric identifiers that can be used for the automated or semi-automated recognition of an individual.[117] In response to the comments, the Commission has decided to change the word "including" in the proposed provision to the phrase "such as" in the final Rule.[118] The comments received have also persuaded the Commission not to include

[114] *See, e.g.*, SIIA, at 4 (suggesting proposed language would potentially apply to skills assessments, time spent, and other usage information that is derived from voice data and used in literacy products with a recording feature); ACT | The App Association, at 4 (suggesting many apps collect voice, fingerprints, and facial features for beneficial uses and mentioning apps assisting autistic children with speech); CARU, at 3 (suggesting "data derived from voice data, gait data, or facial data" is integral to virtual reality products, connected toys, and metaverse experiences); kidSAFE, at 4 (suggesting derived data language is overbroad and could apply to the collection of non-identifying data in virtual reality games, phonics instructional tools, and connected toy devices); R Street Institute, at 1-2 (discussing beneficial use cases such as voice-activated digital assistants with parental controls, educational products, and products assisting children with disabilities).

[115] *See, e.g.*, ConnectSafely, at 1 (emphasizing all users should have access to biometric security tools); IEEE Learning Engineering Consortium, at 5 (encouraging the Commission to consider beneficial uses such as security when determining which biometric identifiers to include in the definition).

[116] *See, e.g.*, NCTA, at 6 ("This definition conflicts with state biometric laws, which consider derived data to be biometric information only where it is used or intended to be used to identify a specific individual."); CCIA, at 3 (discussing conflict with approach to voice recordings in the 2024 NPRM).

[117] 89 FR 2034 at 2042.

[118] At least one commenter suggested adjusting the definitional language to clarify the intended scope of the provision. *See* CIPL, at 5 (suggesting the Commission replace term "including" with the phrase "includes but is not

the proposed language of "data derived from voice data, gait data, or facial data" in the final Rule because it may be overly broad and include some data that cannot currently be used to identify and contact a specific individual. The Commission's original intent in proposing "data derived from voice data, gait data, or facial data" was to cover situations such as where imagery of a biometric characteristic (*e.g.*, a fingerprint or a photograph) is converted into templates or numeric representations such as fingerprint templates or facial templates that can be used to identify and contact a specific individual.[119] The Commission still intends for the modified provision to apply to such biometric identifiers. To make this clearer, and to exclude derived data that cannot be used to identify an individual, the Commission has decided to remove the originally proposed language at the end of the biometric identifier provision but to include additional examples of some covered biometric identifiers that can be used to identify a specific individual such as voiceprints, facial templates, faceprints, and gait patterns.

The Commission has carefully considered input from commenters emphasizing that biometric identifiers are important for uses such as identity authentication, security, age assurance, and virtual reality, and that expanding the definition of personal information to include biometric identifiers will make it more burdensome for operators to collect and use such data from children because they will need to notify parents and obtain verifiable parental consent. However, the Commission is persuaded that enabling parents to make decisions about whether operators are collecting and using their children's biometric identifiers for any purpose

limited to"). The Commission has concluded that an alternative approach of enumerating a complete list of covered biometric identifiers in the Rule would not provide the flexibility necessary to respond to the rapid pace of technological development in biometric recognition.

[119] *See* NIST, The Organization of Scientific Area Committees for Forensic Science, *OSAC Lexicon* (defining the term template in facial identification as a set of biometric measurement data prepared by a facial recognition system from a facial image) (citing ANSI/ASTM Standard Terminology for Digital and Multimedia Evidence Examination), available at *https://www.nist.gov/glossary/osac-lexicon?k=&name=template&committee=All&standard=&items_per_page=50#top*.

and the other benefits commenters identified associated with restricting the collection of children's biometric identifiers without parental consent outweigh the attendant burdens imposed on operators.[120]

c. NPRM Questions Related to "Personal Information"

i) Potential exceptions related to biometric data

The Commission also solicited comments about whether it should consider establishing any exceptions to Rule requirements with regard to biometric data, such as when such data is promptly deleted.[121] In the event that the Commission decided to add biometric identifiers to the definition of personal information, some industry commenters expressed support for adding an exception when there is prompt deletion of biometric data.[122] These commenters suggested this would facilitate beneficial uses such as permitting use of biometric identifiers for identity verification or age assurance purposes.[123]

Other commenters opposed creating any exceptions tied to prompt deletion of biometric identifiers.[124] One consumer group commenter expressed concerns about operators

---

[120] *See* Consumer Reports, at 5 (arguing parents should know and have a choice when operators want to collect or process data about their child's most personal attributes, even if such activities are ephemeral). Importantly, the provision advances two of the goals for the COPPA statute identified in relevant legislative history: (1) enhancing parental involvement in a child's online activity to protect the privacy of children in the online environment, and (2) protecting children's privacy by limiting the collection of personal information from children without parental consent. 144 Cong. Rec. S12741-04, S12787 (1998) (statement of Senator Bryan).

[121] 89 FR 2034 at 2070 (Question 5).

[122] *See, e.g.*, The Toy Association, at 3; Google, at 3; ITIC, at 2; Chamber, at 9; CCIA, at 3. For example, one industry commenter opposed including derived data in any definition related to biometric information and suggested a carveout for biometric data when an identifier is not used to identify a specific individual and is deleted promptly after collection. Epic Games, at 7. Another commenter that opposed the Commission's proposed inclusion of a biometric identifier provision in the definition of personal information also expressed support for a prompt deletion exception permitting use of biometric identifiers for purposes such as fraud and abuse prevention, complying with legal or regulatory requirements, service continuity, and ensuring the safety and age-appropriateness of the service. SIIA, at 15.

[123] *See, e.g.*, Google, at 3; Yoti, at 4-5; SIIA, at 15. *See also* Epic Games, at 8 (recommending adoption of a carveout that would preserve operators' ability to offer features such as motion capture that rely on limited biometric data to translate users' movements to animate non-realistic in-game avatars).

[124] *See, e.g.*, Children's Advocates Coalition, at 58; State Attorneys General Coalition, at 3; Consumer Reports, at 4-5.

"implementing narrow deletion practices, while retaining the ability to use and disclose biometric information for secondary purposes."[125] Another commenter opposing the idea of a deletion exception emphasized the difficulty in verifying operators' compliance with their deletion obligations and suggested that some operators would be incentivized to retain biometric identifiers for their business models.[126] A coalition of state attorneys general suggested that the "mere fact that the data is collected and temporarily held makes it vulnerable to potential cybersecurity attacks or misuse."[127] A public advocacy group commenter also contended it would be premature to adopt a new exception for biometric data based on the limited factual record in this rulemaking proceeding and suggested the Commission should instead consider adding to § 312.12 of the Rule a new voluntary approval process for biometric-related exception requests.[128]

A number of commenters suggested the Commission should consider exceptions for biometric identifiers that are based on specific use cases, such as when fingerprints or facial data are used for security or authentication purposes.[129] One FTC-approved COPPA Safe Harbor

[125] Children's Advocates Coalition, at 65.
[126] Internet Safety Labs, at 4. The Commission's enforcement experience suggests that these concerns are well-founded. *See, e.g.*, Complaint, *In re Everalbum, Inc.*, Dkt. No. C-4743, available at https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_complaint_final.pdf; Complaint, *United States v. Amazon.com, Inc. et al.*, Case No. 2:23-cv-00811 (W.D. Wash. May 31, 2023), available at https://www.ftc.gov/system/files/ftc_gov/pdf/Amazon-Complaint-%28Dkt.1%29.pdf.
[127] State Attorneys General Coalition, at 3.
[128] ACLU, at 15 ("Creating exceptions to the Rule's protections for biometrics should be done on a case-by-case basis with a robust factual record; it is thus better suited for the voluntary approval process rather than ordinary rulemaking.").
[129] *See, e.g.*, ConnectSafely, at 1 ("We strongly believe that biometric tools such as fingerprint and facial recognition should be available for all users to make sure that children and teens, as well as adults, are able to access services in the most secure way possible."); M. Bleyleben, at 2 ("The decision whether or not to make an exception for biometric data that has been promptly deleted should be based on the use case, not solely on whether it has been deleted. For example, using biometrics for platform-based authentication (such as iPhone's face ID) is a positive use case that should be covered under any exception."); IEEE Learning Engineering Consortium, at 5 (suggesting the Commission consider the context in which biometric data is collected and used and that use for security purposes might be treated differently under the COPPA Rule than biometric data used for tracking or monitoring behavior). Another commenter that generally opposed the Commission's proposed biometric identifier provision expressed support for a "prompt deletion" exception permitting the use of biometric identifiers for compliance purposes such

program supported excepting the collection and use of biometric data for security purposes or for a limited purpose such as the temporary use of facial images for age verification or obtaining verifiable parental consent, followed by the data's prompt deletion.[130]

After carefully considering the record and comments related to this question, the Commission has decided not to add any additional exceptions to COPPA Rule requirements related to biometric data at this time, other than the exception to prior parental consent set forth in proposed § 312.5(c)(9) in the 2024 NPRM for the collection of audio files containing a child's voice. The Commission has carefully considered the input from commenters emphasizing that biometric identifiers are important for uses such as identity authentication and security purposes, age assurance, and virtual reality, and that expanding the definition of personal information to include biometric identifiers will make it more burdensome for operators to collect and use such data from children.[131] While technologies utilizing biometrics are developing rapidly, they still vary in terms of efficacy across use cases and across providers. Based on the current record, and in light of the uniquely personal and immutable nature of biometric identifiers and potential privacy and other harms when such data is misused, the Commission has concluded at this time that the impact on such uses and the burden placed on operators to obtain verifiable parental consent are outweighed by the benefit of providing greater protection for this sensitive data and enhancing control for parents. Further, as some commenters noted, storage of sensitive biometric identifiers for even limited periods of time increases the risk that such data will be compromised in a data security incident.

---

as to facilitate "fraud and abuse prevention, complying with legal or regulatory requirements, service continuity, and ensuring the safety and age-appropriateness of the service." SIIA, at 15.

[130] kidSAFE, at 4.

[131] The Commission notes this burden is only imposed on operators of child-directed websites or online services and entities that have actual knowledge they are collecting personal information from users of a child-directed site or service.

ii) Government-issued Identifiers

The Commission also requested comment on whether it should revise the definition of "personal information" to specifically list government-issued identifiers beyond Social Security numbers that are currently included in the definition.[132] The Commission received relatively few comments addressing this proposal, and all of them supported listing additional government-issued identifiers in the definition of "personal information."[133]

One commenter noted such identifiers are likely already covered under the existing definition of personal information, but suggested that adding an explicit provision for government-issued identifiers would provide greater clarity.[134] A coalition of state attorney generals expressed the view that parents should have the right to review and to have discussions with their children before these highly sensitive identifiers are shared.[135] Based on the comments and its enforcement experience, the Commission is persuaded that government-issued identifiers can be used to identify and permit the physical or online contacting of a specific child and has concluded that it would be beneficial to expressly incorporate additional government identifiers in the definition of personal information in order to provide greater clarity. Therefore, paragraph 6 of the current definition of "personal information" which is "a Social Security number" will be amended to: "[a] government-issued identifier, such as a Social Security, state identification card, birth certificate, or passport number." The Commission notes that the list of examples of specific government identifiers is not intended to be exhaustive.

---

[132] 89 FR 2034 at 2070 (Question 7).
[133] *See* State Attorneys General Coalition, at 4 (recommending inclusion of passport and passport card numbers, Alien Registration numbers or other identifiers from United States Citizenship and Immigration Services, birth certificate numbers, identifiers used for public benefits, state ID card numbers, and student ID numbers); Consumer Reports, at 5-6 (suggesting inclusion of passport, birth certificate, and DMV-issued Child ID cards); EPIC, at 4 (expressing general support for including government-issued identifiers); Common Sense Media, at 7 (same); AASA, The School Superintendents Association, at 8 (same).
[134] Consumer Reports, at 6.
[135] State Attorneys General Coalition, at 4.

iii) Screen and User Names

Since the 2013 Amendments to the Rule, the definition of personal information has included screen or user names to the extent that these identifiers function in the same manner as "online contact information." In the 2024 NPRM, the Commission sought comment on whether screen or user names should also be treated as online contact information or personal information if the screen or user names do not allow one user to contact another user through the operator's website or online service, but could enable one user to contact another by assuming that the user to be contacted is using the same screen or user name on another site or service.[136]

A minority of commenters expressed support for this suggestion.[137] Some of these commenters suggested there is frequent reuse of screen and user names across platforms, and that screen and user names might allow entities to link information collected across various platforms.[138] Another commenter cited safety concerns and suggested screen and user names can facilitate contact with, and the grooming of, children for sexual exploitation or other harms.[139]

A majority of commenters opposed this proposal for a variety of reasons.[140] Some of these commenters argued that the proposal to expand the definition is inconsistent with the COPPA statute because a screen or user name does not necessarily permit the physical or online contacting of a specific individual.[141] Opponents also highlighted practical problems associated with such an expansion. For example, commenters suggested the proposal would likely result in

[136] 89 FR 2034 at 2070 (Question 4.a).
[137] Internet Safety Labs, at 3; AASA, The School Superintendents Association, at 8; ACLU, at 9-10; Center for AI and Digital Policy, at 2-3; Consumer Reports, at 3-4.
[138] *See, e.g.*, Parent Coalition for Student Privacy, at 3,7; Consumer Reports, at 3-4; AASA, The School Superintendents Association, at 8.
[139] Center for AI and Digital Policy, at 2-3.
[140] *See, e.g.*, Chamber, at 2-3; ESRB, at 23-25; ESA, at 8; IAB, at 5-6; kidSAFE, at 2-3; M. Bleyleben, at 2; CCIA, at 4, The Toy Association, at 3-4; Privacy for America, at 15-16; Epic Games, at 8-9.
[141] *See, e.g.*, ESA, at 8; CCIA, at 4. At least one industry commenter contended that it is common for the same screen name or user name to be used by different children. *See* The Toy Association, at 3.

operators treating all screen and user names as personal information because of the difficulty in determining whether a particular child has used the same screen or user name on other sites or services.[142] Many commenters emphasized this result would adversely impact privacy interests of children and parents because it would require operators of websites or online services that do not currently collect personal information from children to need to do so in order to seek verifiable parental consent.[143] Industry commenters also opined that the suggested expansion of screen and user names constituting personal information would require significant changes to common business practices and would impose significant burdens on operators related to changing such practices and trying to determine whether screen or user names are being re-used on other sites and services in ways that permit communication.[144]

The Commission currently does not have sufficient evidence concerning either the extent to which children are currently reusing their screen and user names across platforms or the prevalence of children being contacted via screen or user names through secondary platforms to warrant amending the Rule.[145] Recognizing the difficulties operators might face in determining whether screen and user names are being used by specific individuals on other websites and online services, the Commission is persuaded that amending the Rule now to require operators to treat screen or user names that do not allow one user to contact another user through the

[142] IAB, at 5; ESA, at 9.
[143] For example, the U.S. Chamber of Commerce suggested many operators collect an anonymous username or screen name precisely to avoid collecting personal information — such as full name or email address — when such information is not otherwise needed and that a change to the definition would require operators to collect more personal information from children and their parent to seek verifiable parent consent. Chamber, at 2-3. *See also* ESRB, at 23-24; ESA, at 8; IAB, at 5-6; The Toy Association, at 3-4; Privacy for America, at 16; Epic Games, at 8.
[144] *See, e.g.*, IAB, at 5 (suggesting operators cannot reasonably determine whether a particular child has used the same screen or user name across different sites or service); Epic Games, at 8 (stating that video game companies use anonymous screen and user names in many ways that do not facilitate the contacting of an individual in order to protect user privacy and arguing that it would be burdensome to require operators to monitor use of their screen names on third-party sites and services).
[145] *See* kidSAFE, at 2-3 (stating that it was not aware of any studies indicating children are using the same exact usernames across multiple online services, such that knowing a child's username on one online service would allow for direct communication on another online service).

operator's website or online service as personal information would likely cause operators to treat all screen and user names as personal information and have negative privacy consequences, including increased data collection by operators that currently do not need to collect personal information.[146] After carefully considering the record and comments, the Commission has therefore concluded that it will not amend the definitions of personal information or online contact information at this time to include the suggestion discussed in Question Four of the "Questions for the Proposed Revisions to the Rule" section of the 2024 NPRM. The Commission notes that if a screen or user name collected online from a child is combined with other personal information, then it is considered personal information under the provision set forth in paragraph 10 of the Rule's definition of "personal information."

iv) Avatars

The Commission solicited comments in Question Six of the "Questions for the Proposed Revisions to the Rule" section of the 2024 NPRM about whether an avatar generated from a child's image should constitute personal information under the Rule 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, and, if so, whether the current Rule provides sufficient coverage or whether further modifications to the definition of personal information are necessary to ensure coverage.[147]

[146] *See* ESA, at 8 (suggesting that restricting the use of anonymous screen names and user names would negatively impact the online experience for children and undermine the data minimization principles underlying COPPA and stating that many screen and user names are automatically generated and assigned by the service, and therefore would be unlikely to allow a user to contact another user on another website or online service).
[147] 89 FR 2034 at 2070 (Question 6).

A minority of commenters supported treating avatars based on a child's image as personal information under the circumstances described in Question Six.[148] A coalition of state attorneys general cited concerns about the possibility of reverse engineering from avatars that are generated using biometric data, and recommended amending the definition of personal information to include "an avatar generated on the child's image and likeness, whether or not a photograph, video or audio file is provided or stored."[149] Another commenter suggested that some popular platforms are encouraging the creation of realistic avatars modelled on users' biometric data and expressed concerns about the possibility that companies might "collect data from an avatar to analyze and influence a child's behavior" including through targeted advertising.[150] A consumer group contended that a likeness of a child generated from an image could alone, or when combined with other sources of information, be used to individually identify a child and suggested adding "or likeness of a child" to existing paragraph 8 of the COPPA Rule's personal information definition to provide coverage if the Commission decided not to adopt the NPRM proposal of including "data derived…from facial data" in the biometric identifier provision in the personal information definition.[151]

[148] *See, e.g.*, Consumer Reports, at 5; EPIC, at 3-4 (recommending including avatars generated from a child's image); State Attorneys General Coalition, at 3-4 (same); Common Sense Media, at 13 (supporting adding avatars that are identifiable and are able to be contacted outside of a specific service or session); L. Lu, at 1 (recommending that definition of personal information include identifiable avatars). At least one commenter recommended the Commission treat all avatars as personal information, regardless of whether they are generated from a child's image. *See* Internet Safety Labs, at 4.

[149] State Attorneys General Coalition, at 4 ("If the avatars are based on the child's photograph or likeness, regardless of whether the original source is retained, the avatar could be used in the identification of the child, through many different methods including reverse image searches, facial recognition tools, or combining information gleaned from the avatar with other known elements of personal information.").

[150] L. Lu, at 2.

[151] Consumer Reports, at 5. Paragraph 8 of the COPPA Rule's personal information definition encompasses "[a] photograph, video, or audio file where such file contains a child's image or voice." 16 CFR 312.2.

Another commenter discussed potentially sensitive information that might be derived from avatars such as ethnicity or disability information, but suggested more research should precede expansion of the definition.[152]

For a variety of reasons, a majority of commenters opposed the idea of treating avatars described in Question Six as personal information under the Rule.[153] Some of these commenters emphasized that avatars are often temporary, changeable, and not linkable to personal information.[154] Many commenters raised statutory concerns about expanding the definition of personal information to include avatars, arguing that avatars are not individually identifiable and cannot be used for the physical or online contacting of a child.[155] Some commenters suggested that if a photograph used to generate an avatar is processed locally on a device, the photograph and the avatar would be outside the scope of the COPPA statute and Rule because the photograph is not information collected or stored online.[156] Several commenters argued the proposal would be inconsistent with existing FTC guidance permitting operators to blur the facial features in children's photos before posting the photos online in order to avoid collecting

[152] Yoti, at 5 ("An avatar could give evidence or clues as to age, gender, disability, ethnicity… If the avatar could be combined with additional information held by a service provider, to reasonably identify the avatar's human representative, that could pose greater risks to a minor….").
[153] *See, e.g.*, The Toy Association, at 3-4; ITIC, at 2-3; ESA, at 11-12; ESRB, at 25; Kidentify, at 3-4; Epic Games, at 9-10.
[154] *See* ITIC, at 3. *See also* Kidentify, at 4 (suggesting that avatars are rarely actually used in practice to identify or contact an individual in-game due to their frequently changing nature); CARU, at 7 (suggesting that avatars vary widely, and that many users do not base avatars on their own images); ACT | The App Association, at 5 (contending that avatars are temporary and alterable representations that often do not reflect personal characteristics of an individual user and do not enable contact).
[155] *See, e.g.*, ITIC, at 3; SIIA, at 5, 15; IAB, at 7-8; Chamber, at 2; ACT | The App Association, at 5.
[156] ESA, at 11-12 ("[I]f the photograph of the child is not uploaded to the site or service, the photograph is processed locally on the device to generate the avatar. The FTC has previously recognized that local processing of a child's personal information does not trigger COPPA because the statute requires that personal information must be collected, used, or stored over the Internet."). *See also* Chamber, at 2 (suggesting that if an avatar image does not leave the device, no personal information is collected under COPPA); IAB, at 7 (same).

personal information.[157] Commenters contended that avatars similarly obscure individually identifying information and should not be treated as personal information.[158]

Industry commenters also raised practical and policy-related objections to the idea of requiring operators to treat avatars generated from a child's image, in situations where the operator has not itself collected the child's photograph, as personal information. For example, commenters suggested that expanding coverage for avatars under the Rule would be burdensome and confusing, and introduce significant compliance challenges, particularly because operators that do not collect photographs or videos of users would have difficulty determining whether an avatar is created from a child's image.[159] Commenters suggested that such uncertainty would deter online service providers from offering avatar-based features in games and related product offerings, and that this would negatively impact users' privacy and online experiences.[160] Commenters argued that the use of avatars as online proxies is privacy-enhancing because they can, like screen and user names, be used by online services as a substitute for personal identification.[161] Several commenters also urged the Commission to consider that avatars also benefit users by personalizing online experiences and allowing users to explore self-expression online.[162]

After carefully considering the record and comments, the Commission is persuaded that it would likely be difficult for operators to determine whether an avatar is generated from a child's

[157] *See, e.g.*, ESA, at 12; NCTA, at 7. These commenters cited staff guidance in COPPA Frequently Asked Questions, Section F.3, and previous statements in the 2013 Statement of Basis and Purpose. *See* COPPA FAQs, FAQ Section F.3; 78 FR 3972 at 3982 n. 123.
[158] *See, e.g.*, NCTA, at 7 (suggesting that "avatars, even if initially generated from a child's image, once altered do not constitute an identity of the sort that permits physical or online contacting of a child"); ESA, at 12 (contending that "once a photo has been transformed into an avatar, facial recognition technology no longer is able to identify the specific individual").
[159] *See, e.g.*, CARU, at 7; ITIC, at 3; Kidentify, at 3.
[160] *See, e.g.*, Kidentify, at 3-4; CARU, at 7.
[161] *See, e.g.*, M. Bleyleben, at 3; IAB, at 7-8; The Toy Association, at 3-4; SIIA, at 5; NCTA, at 6; Chamber, at 2; SuperAwesome, at 5.
[162] L. Lu, at 1; The Toy Association, at 3-4; ITIC, at 2-3; Chamber, at 2-3; SuperAwesome, at 5.

image in situations where they have not collected an image of the child. For example, with the advent of generative AI, the Commission expects that it would be possible for a user to create a highly realistic avatar that might appear to be generated from a child's image. The Commission also does not currently have sufficient evidence that avatars are individually identifying. Indeed, a number of the comments received suggest that avatars are often temporary and may not resemble users.[163] However, the Commission notes that an avatar that the operator collects online from a child and combines with another identifier included in the definition of personal information is personal information pursuant to paragraph 10 of the Rule's definition of personal information.[164] The Commission further notes that it will continue to monitor marketplace and technological developments in this area and may revisit Rule amendments related to avatars in the future.[165]

v) Information Concerning the Child or the Parents of that Child

The definition of personal information in the current Rule includes "information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in [the Rule's definition of "personal information]."[166] This provision includes the same language found in the COPPA statute's definition of personal information.[167] In the 2024 NPRM, the Commission solicited comments about whether the

[163] *See, e.g.*, M. Bleyleben, at 3; Kidentify, at 4; CARU, at 7; ACT | The App Association, at 5.
[164] *See* FTC Press Release, *FTC Will Require Microsoft to Pay $20 million over Charges it Illegally Collected Personal Information from Children without Their Parents' Consent* (June 5, 2023), available at *https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-will-require-microsoft-pay-20-million-over-charges-it-illegally-collected-personal-information* (discussing applicability of COPPA to avatars generated from a child's image when combined with other personal information).
[165] It is possible that if cross-platform use of avatars becomes common, avatars could be used to identify and contact specific individuals and track users across domains. *See* M. Bleyleben, at 3.
[166] 16 CFR 312.2.
[167] 15 U.S.C. 6501(8)(G).

phrase "concerning the child or the parents of that child" in the Rule requires further clarification.[168] The Commission received relatively few significant comments.

A coalition of state attorneys general suggested the Commission consider amending this provision to: "information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in [the Rule's definition of 'personal information'], or which may otherwise be linked or reasonably linkable to personal information of the child."[169] In response, the Commission observes this provision already provides broad coverage for information concerning children and parents that the operator collects online from a child when it is combined with identifiers included in the Rule's definition of personal information and declines to expand coverage to the extent proposed by this commenter.

A number of commenters asked the Commission to clarify when, or if, inferred data would be considered personal information under the provision in paragraph 10 of the Rule's definition of personal information.[170] One consumer group stated that it disagreed with the Commission's earlier conclusion in the 2024 NPRM that inferred data is outside the scope of the COPPA statute[171] and urged the Commission to state specifically that information inferred about a child is information "concerning the child."[172] This commenter noted that inferred data is commonly used to categorize individuals for marketing purposes and suggested parents should

[168] 89 FR 2034 at 2070 (Question 8).
[169] State Attorneys General Coalition, at 5. *See also* SIIA, at 9 (suggesting the word "concerning" is potentially overbroad and recommending adding language to the provision to limit coverage to data that is "linked or reasonably linkable" to the child or parents of that child).
[170] *See, e.g.*, CDT, at 5-6; CIPL, at 5; IAB, at 8-9.
[171] *See* 89 FR 2034 at 2042 ("The Commission has decided not to propose including inferred data or data that may serve as a proxy for 'personal information' within the definition … [T]o 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.").
[172] Consumer Reports, at 6.

have the right both to be notified when this information is generated and to delete such information when the disclosure of a "business' assumptions about a child carry the risk for personal embarrassment, social stigmatization, [or] discrimination, [and] could be used as a basis to make legal or other similarly significant decisions."[173]

Several industry commenters asked the Commission to confirm that the catch-all provision in paragraph 10 of the definition of personal information does not extend to inferred data.[174] Others expressed concern about potential interference with the support for the internal operations exception if inferred data not collected from a child and linked to persistent identifiers were to be covered by the catch-all provision.[175] To clarify that inferred information can be combined with persistent identifiers to support the internal operations of a site or service without parental consent, some commenters suggested amending the catch-all provision in the Rule's definition of personal information to "information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition, except to the extent such information is combined with a persistent identifier and used solely to support internal operations."[176]

After carefully considering the record and comments related to this question, the Commission has decided to retain the existing language in paragraph 10 of the Rule's definition of personal information, which tracks the definition in the COPPA statute and provides broad coverage for a wide range of information that is collected from children when such information

[173] *Id.*
[174] *See, e.g.*, ESA, at 12 (urging Commission to clarify a statement in the 2024 NPRM suggesting that inferred data could fall within COPPA's catch-all provision if combined with other identifiers listed in the definition of personal information and arguing that inferred data does not fall under the catch-all provision if it is not collected from a child online); CIPL, at 5 (same); CDT, at 5-6 (asking the Commission to clarify when and how the catch-all provision applies to inferred data).
[175] *See, e.g.*, Chamber, at 4; ESA, at 12-13.
[176] *See* Epic Games, at 10; ESA, at 12-13.

is combined with other identifiers set forth in the definition.[177] While the Commission agrees that inferred or proxy data about a child may sometimes include sensitive information presenting privacy risks, the COPPA statute regulates the collection of personal information from a child,[178] and inferred or proxy data that is derived from information collected from sources other than a child therefore cannot be treated as personal information under the COPPA statute.

d. The Commission Adopts Amendments Regarding "Personal Information"

As discussed *supra*, after carefully considering the record and comments, the Commission is adopting an amended version of the biometric provision proposed in the 2024 NPRM to be included in the definition of personal information. Specifically, the Commission has decided not to include the language "data derived from voice data, gait data, or facial data" in the provision for the reasons discussed in Part II.B.3.b. The Commission has also decided to replace the word "including" with "such as" and to provide additional illustrative examples of biometric identifiers to provide further clarity concerning the provision's coverage. The language the Commission is adopting for the biometric identifier provision in the final Rule's definition of personal information includes the following: "A biometric identifier that can be used for the automated or semi-automated recognition of an individual, such as fingerprints; handprints; retina patterns; iris patterns; genetic data, including a DNA sequence; voiceprints; gait patterns; facial templates; or faceprints[.]" As discussed in Part II.B.3.c.ii, the Commission has also decided to amend paragraph 6 of the definition of personal information to include "[a]

[177] *See* 64 FR 59888 at 59892 (definition of personal information covers "non-individually identifiable information (e.g., information about a child's hobbies or toys) that is associated with an identifier").
[178] *See* 15 U.S.C. 6502(a)(1).

government-issued identifier, such as a Social Security, state identification card, birth certificate, or passport number[.]"

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

a. The Commission's Proposal Regarding "Support for the Internal Operations of the Website or Online Service"

The current Rule defines "support for the internal operations of the Web site or online service" to include seven enumerated activities and further provides that the information collected to perform such 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."[179] In the 2024 NPRM, the Commission proposed two substantive amendments to the definition's use restriction. First, the Commission proposed an amendment clarifying that the information collected for the enumerated activities in the definition may be used or disclosed to carry out those activities.[180] Second, the Commission proposed expanding the non-exhaustive list of use restrictions in the definition to prohibit operators relying on the support for the internal operations exception to the COPPA Rule's verifiable parental consent requirement from using or disclosing personal information to contact a specific individual "in connection with processes

[179] 16 CFR 312.2, definition of "support for the internal operations of the Web site or online service." In adopting the 2013 Amendments to the Rule, the Commission observed that a number of functions fall within the scope of the enumerated activities in the definition of "support for the internal operations of the Web site or online service." Specifically, the Commission recognized that "intellectual property protection, payment and delivery functions, spam protection, optimization, statistical reporting, or de-bugging" are covered by the definitional language permitting activities that "maintain or analyze" the functioning of the website or online service or those that protect the "security or integrity" of the website or online service. 78 FR 3972 at 3981. In the 2024 NPRM, the Commission explained its reasons for declining to expand or narrow the list of activities included in the definition as suggested by some commenters. 89 FR 2034 at 2044-2045. The Commission also clarified that ad attribution, personalization, product improvement, and fraud prevention fall within the scope of the activities already enumerated in the definition. 89 FR 2034 at 2045.

[180] 89 FR 2034 at 2050. *See also id.* at 2045.

that encourage or prompt use of a website or online service."[181] The Commission also solicited comments about "whether and how the Rule should differentiate between techniques used solely to promote a child's engagement with the website or online service and those techniques that provide other functions, such as to personalize the child's experience on the website or online."[182]

b. Public Comments Received in Response to the Commission's Proposal Regarding "Support for the Internal Operations of the Website or Online Service"

The Commission received at least one comment supporting the first proposed amendment to the definition of "support for the internal operations of the website or online service."[183] and did not receive any comments objecting to it. The Commission received a number of comments both for and against the proposal to expand the non-exhaustive list of use restrictions in the definition to include efforts to contact a specific individual "with processes that encourage or prompt use of a website or online service."

[181] *Id.* at 2072. *See also id.* at 2045.
[182] *Id.* at 2046, 2070-71 (Question 15). Commenters suggested various alternatives to the proposed amendment that are responsive to this question. For example, an FTC-approved COPPA Safe Harbor program urged the Commission to drop the proposed restriction or adjust it in a way that distinguishes "between engagement techniques that are intrusive, misleading, or unexpected, versus ones that are reasonable and/or core to the functioning of the service" and specifically suggested the alternative language of "in connection with processes that encourage or prompt *continuous* use of a website or online service *in a manner not core to the function of the service or not reasonably expected by the user*, or for any other purpose." kidSAFE, at 6 (emphasis in original). An industry commenter contended that "engagement techniques falling outside the Support for Internal Operations exception should be restricted to practices that have negative consequences for children, rather than restricting things that simply make a service more relevant for them, notify them of rewards, or even promote an age-appropriate experience." Chamber, at 5. Another industry commenter that objected to changing the definition suggested in the alternative that the Commission "should clarify that these restrictions do not apply to techniques used to drive engagement for purposes that benefit children … and personalization that seeks to make a service more relevant." Google, at 10. In response, the Commission notes that it believes such alternatives would introduce considerable uncertainty given the variation in possible conclusions as to whether, for example, a prompt is intrusive or has a negative consequence and would be difficult for the Commission to enforce for the same reason.
[183] *See* CIPL, at 6.

A number of consumer advocacy groups, school-related groups, governmental commenters, and other commenters supported the proposal to restrict the use of persistent identifiers collected under the support for the internal operations exception to COPPA's verifiable parental consent requirement to contact a specific individual in order to encourage or prompt use of a website or online service.[184] For example, commenters supporting the additional restriction contended it is necessary to address the use of engagement techniques that exploit children's developmental vulnerabilities[185] and the potential adverse impacts on mental health associated with children spending extended periods of time online or engaging with social media platforms.[186] At least one commenter suggested that parents should be given the opportunity to decide whether to consent to the use of their children's personal information to feed features that encourage engagement with websites or online services.[187] Other supportive commenters contended that using children's personal information to encourage or prompt use of a website or online service would be inconsistent with the intended purpose of the support for the internal operations exception.[188] Other commenters, while generally supporting the Commission's

[184] *See, e.g.*, S. Winkler, at 1-2; Children and Screens, at 2; NYC Technology and Innovation Office, at 2-3; Mental Health America, at 1-2; ASSA, The School Superintendents Association, at 5; SuperAwesome, at 4; Motley Rice, at 13; Sandy Hook Promise, at 5; Children's Advocates Coalition, at 29-31; Family Online Safety Institute, at 2-3; Data Quality Campaign, at 4; Anonymous, Doc. FTC-2024-0003-0125, at 1; Anonymous, FTC-2024-0003-0127, at 1.

[185] *See, e.g.*, Children's Advocates Coalition, at 29 ("[E]ngagement-maximizing techniques pose particular risks when used on minors, who are developmentally vulnerable to features and functions designed to extend their use of a website or service.").

[186] *See, e.g.*, S. Winkler, at 1-2; Children and Screens, at 2; Data Quality Campaign, at 4; Mental Health America, at 1-2.

[187] S. Winkler, at 1-2.

[188] *See, e.g.*, Children and Screens, at 2 (suggesting "[s]uch uses are an abuse of the exception…."); Children's Advocates Coalition, at 29 (contending children's "nascent executive function skills related to 'impulse control, decision-making, attentional flexibility, planning, self-regulation'…make it particularly difficult for children to resist prompts to return to or stay on a platform" and suggesting that "[u]sing a child's personal data to exploit these vulnerabilities via notifications or nudges exceeds the limited practical purposes for which the internal operations exception is intended") (internal citation omitted). As part of the 2013 Amendments to the Rule, the Commission explained that the support for the internal operations exception reflects the agency's recognition that "persistent identifiers are [] used for a host of functions that have little or nothing to do with contacting a specific individual, and that these uses are fundamental to the smooth functioning of the Internet, the quality of the site or service, and the individual users' experience." 78 FR 3972 at 3980.

proposal, suggested push notifications and prompts encouraging children to use a website or online service should be permissible in certain settings, such as "to promote pedagogical engagement on edtech platforms."[189]

For a variety of reasons, a majority of commenters that weighed in on this proposal, representing different types of stakeholders, opposed amending the definition's use restriction to prohibit operators from relying on the support for the internal operations exception when persistent identifiers are being used in connection with processes that encourage or prompt the use of a website or online service.[190] Several industry group commenters suggested the proposal falls outside the scope of the objectives that the COPPA statute was intended to address and exceeds the Commission's statutory authority.[191]

---

[189] ASSA, The School Superintendents Association, at 5. *See also* Advanced Education Research and Development Fund, at 7. Some commenters opposing the proposal raised similar concerns about the importance of avoiding amendments to the Rule that would interfere with beneficial features of ed tech products or services. *See, e.g.*, Google, at 10 (discussing ed tech and language learning products and arguing the proposed change should not apply to "techniques used to drive engagement for purposes that benefit children (e.g., sending them important reminders) and personalization that seeks to make a service more relevant."); SIIA, at 6 (contending that "machine learning 'prompting' or 'nudging'" may be beneficial in some circumstances such as "algorithmic or machine learning prompts for the purposes of meeting learning objectives … in the context of education technology (specifically adaptive and/or personalized learning)").

[190] *See, e.g.*, SIIA, at 5-6, 16; Chamber, at 5; ACLU, at 21-22; ESA, at 16-18; IAB, at 18-20; NCTA, at 13-14; ACT | The App Association, at 7-8; Scalia Law School Program on Economics & Privacy and University of Florida Brechner Center, at 5-6; kidSAFE, at 5-6; ANA, at 14-15; CCIA, at 5; Google, at 9-10; The Toy Association, at 2-3; Future of Privacy Forum, at 8-9.

[191] *See, e.g.*, Google, at 9-10 ("None of the objectives that COPPA was designed to achieve, or harms that COPPA was intended to prevent, have anything to do with children's engagement with online content. The FTC's attempt to regulate children's engagement with content through the COPPA Rule goes beyond its statutory authority and is the type of value judgment that is appropriately reserved for Congress."); Chamber, at 5 (suggesting "it is not clear that COPPA confers authority on the FTC to propose this restriction"); ESA, at 18 ("The intent of COPPA was not to regulate how operators design experiences for children online beyond the specific requirements related to the processing of children's personal information. The FTC should not use this rulemaking to implement age-appropriate-design-code-style features that would overstep its statutory authority and congressional intent in order to, for example, restrict the amount of time children spend online."); IAB, at 19 ("COPPA is intended to protect the privacy and safety of children's personal information online, not to be a 'design code' statute."); NCTA, at 14 (arguing that proposal is "outside the scope of COPPA's remit, which is to protect *privacy* of children online") (emphasis in original).

Several commenters asserted the proposed language is vague or overbroad and fails to give operators adequate notice of the prohibited conduct.[192] Another commenter suggested the proposed language is "potentially broader than the concerns of maximizing user engagement and could include something as infrequently as one notification per day."[193] Other commenters argued the proposed restriction is broad enough to potentially include any design feature improving the user experience, because a streamlined or personalized user experience could be viewed as encouraging or prompting the use of the service.[194]

Many commenters emphasized that the proposed restriction could have unintended consequences, such as preventing operators from using prompts and notifications that are beneficial for children.[195] For example, commenters mentioned features in educational products that rely on push notifications to help children remain focused on studies or notifications to

[192] *See, e.g.*, ESA, at 16 (suggesting language "does not clearly indicate the type of functions and features that are prohibited by the proposed restriction" and therefore does not provide adequate notice to operators about what is prohibited); NCTA, at 14 (contending proposal is vague and unenforceable); kidSAFE, at 5 (arguing restriction is too broad and may require operators to obtain verifiable parental consent and increase data collection "for prompts that are essential to the core function of child-directed services and reasonably expected by users of those services"); IAB, at 18-19 ("[T]he 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."); ANA, at 15 (arguing "proposed restriction is vague and unclear").

[193] Future of Privacy Forum, at 9.

[194] *See, e.g.*, ESA, at 16-17; NCTA, at 14 ("[T]he language could be interpreted that *any* design feature that improves user experience is problematic….") (emphasis in original); Scalia Law School Program on Economics & Privacy and University of Florida Brechner Center, at 6 (suggesting proposal will adversely impact quality of online services for children because "[u]nder the potentially vast and highly subjective standard proposed by the Commission, taking actions to improve one's service risks being deemed by the Commission to have 'encouraged' use or attention"); American Association of Advertising Agencies ("4A's"), at 3 ("The use of persistent identifiers for personalization allows operators to provide valuable benefits to children including reactive learning environments, tailored and improved products, and fraud prevention services. In the longer term, widespread disruption of these services by way of requiring verifiable parental consent would mean a significantly downgraded user experience for children as they engage safely online."); IAB, at 18-19; ANA, at 15 ("On its face, this proposal could restrict *any feature* that makes the offered services more enjoyable or interesting to kids.") (emphasis in original). *See also* NCTA, at 14 ("Even if the FTC's intention is to protect children against dark patterns, addictive features, or other putatively manipulative characteristics and capabilities, the proposed language sweeps far more broadly and threatens to interfere with beneficial capabilities that enhance user experience.").

[195] *See, e.g.*, SIIA, at 6, 19-20 (suggesting proposal would prohibit useful notifications and machine learning-based prompts reminding students to complete lessons or homework); Chamber, at 5; IAB, at 18-19; ACT | The App Association, at 7-8; CIPL, at 6 (requesting clarification of the terms used in proposal and suggesting undefined phrase of "'encourage or prompt use'…could unwittingly prohibit innovative and beneficial uses for end users…").

children related to taking turns in an online game.[196] Another commenter opposing the additional restriction urged the Commission to consider positive use cases for prompts such as "reminders about meditation apps, homework assignment reminders, and notifications about language lessons."[197] Another commenter criticized the proposal for failing to "differentiate between features that are: (1) commercial in nature or enable access to third parties and/or harmful content, and (2) [those] intended to helpfully personalize a child's experience."[198]

Other industry and public interest group commenters argued that the proposed use restriction unduly restricts legal speech and may violate First Amendment constitutional protections.[199] At least one public interest group commenter urged the Commission to address the misuse of push notifications through guidance and enforcement rather than with rulemaking and further suggested that changing the Rule to categorically prohibit push notifications would, in some circumstances, be inconsistent with the COPPA statute's requirement that agency regulations permit operators to respond "more than once directly to a specific request from the child" as long as parents are provided with notice and an opportunity to opt out.[200]

---

[196] *See, e.g.*, CCIA, at 5 ("Some educational applications…utilize push notifications to help children remain focused on their studies, including in conjunction with usage 'streaks' and other methods intended to gamify learning for children's benefit."); E. Tabatabai, at 12-13 (stating that ed tech operators often use "benign forms of encouragement to make a learning activity more enjoyable … and to increase the learning benefit for the child by encouraging additional practice"); kidSAFE, at 5-6 (suggesting restriction is overbroad and would apply to beneficial prompts such as (1) an educational website sending alert to student that a teacher has assigned new materials or graded an assignment; (2) a chess game sending an in-app notification that the next move is ready; (3) a connected toy device displaying an indicator that the device is ready to be used after software update or completed battery charge; (4) language learning apps prompting learner to engage in scheduled practice-based curriculum; (5) notice of friend request or that friend request has been accepted; and (6) an email alert informing user to confirm login to account from an unrecognized device).

[197] Future of Privacy Forum, at 9.

[198] ACT | The App Association, at 7-8.

[199] *See, e.g.*, Chamber, at 5; ACLU, at 21; NCTA, at 13 (stating COPPA statute is not an age appropriate design code and that "such efforts at the state level are actively being challenged on constitutional grounds as impermissible restrictions on speech"); ACT | The App Association, at 8 (suggesting regulation of engagement techniques as proposed would restrict access to legal content online and "gives rise to First Amendment concerns"). *See also* ESA, at 18 (contending an "overly broad interpretation of this prohibition could also unconstitutionally limit adults' ability to access online content by making sites and services less easy to use (e.g., by limiting personalization)").

[200] *See* ACLU, at 22 (citing 15 U.S.C. 6502(b)(2)(C)).

c. The Commission Adopts Amendments Regarding "Support for the Internal Operations of the Website or Online Service"

After carefully considering the record and comments, and for the reasons discussed in Part II.B.4.b of this document, the Commission adopts the proposed amendment clarifying that persistent identifiers used for the activities enumerated in paragraphs (1)(i)-(vii) of the definition of "support for the internal operations of the website or online service" may be used or disclosed in connection with those activities.[201]

By contrast, the Commission is persuaded that adding "in connection with processes that encourage or prompt use of a website or online service" to the use restriction as proposed is overly broad and would constrain beneficial prompts and notifications, as well as those that prolong children's engagement with sites and services, in ways that may be detrimental. Although the Commission is not making this proposed change to the Rule, the Commission notes the proposal is consistent with the goals of the COPPA statute, which include protecting children's privacy by "enhancing parental involvement in a child's online activities" and "by limiting the collection of personal information from children without parental consent."[202] The Commission shares supportive commenters' concerns regarding practices that operators employ to maximize children's engagement with online services[203] and notes that it may pursue enforcement under Section 5 of the FTC Act in appropriate cases to address unfair or deceptive acts or practices encouraging prolonged use of websites and online services that increase risks of

[201] *See supra* note 179.
[202] *See* 144 Cong. Rec. S12787-04, S12787 (1998) (statement of Senator Bryan).
[203] *See, e.g.*, FTC Press Release, *FTC Announces Virtual Workshop on the Attention Economy: Monopolizing Kids' Time Online* (Sept. 26, 2024), available at *https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-virtual-workshop-attention-economy-monopolizing-kids-time-online*.

harm to children.[204] The Commission also reiterates that the support for the internal operations exception restricts the use of persistent identifiers, without parental consent, to what is "necessary" for the activities enumerated in paragraphs 1(i)-(vii) of the definition of the "support for the internal operations of the website or online service."[205]

d. NPRM Question Nine: Personalization and "Support for the Internal Operations of the Website or Online Service"

In Question Nine of the "Questions for the Proposed Revisions to the Rule" section of the 2024 NPRM, the Commission noted that some commenters on the 2019 Rule Review Initiation recommended modifications to the "support for the internal operations of the website or online service" definition to limit personalization to "user-driven" actions and to exclude methods designed to maximize user engagement.[206] To follow up on those recommendations, the 2024 NPRM requested comment as to the circumstances under which personalization would be considered "user-driven" versus "operator-driven" and as to how operators use persistent identifiers, as defined by the COPPA Rule, to maximize user engagement with a website or online service.[207]

Most commenters that responded to Question Nine recommended against the Commission amending the definition of "support for the internal operations of the website or online service" to differentiate between user-driven versus operator-driven personalization actions.[208] Some such commenters expressed concern that the meaning of "user-driven"

---

[204] There may be circumstances where the collection of personal information for the purposes of increasing engagement could violate § 312.7 of the COPPA Rule, where an operator conditions a child's participation in an activity on the collection of such information and such information is more than is reasonably necessary to participate in the activity. *See* 16 CFR 312.7.
[205] *See* 16 CFR 312.2.
[206] 89 FR 2034 at 2070.
[207] *Id.*
[208] *See*, *e.g.*, ACLU, at 21-22; Privacy for America, at 14; ANA, at 9; Center for AI and Digital Policy, at 6-7; ESA, at 17; CCIA, at 4-5; SIIA, at 16; News/Media Alliance, at 3; Chamber, at 5; kidSAFE, at 6.

personalization is not clear.[209] Some commenters asserted that an attempt to draw a distinction between user-driven and operator-driven personalization might violate the First Amendment or exceed the Commission's authority under the COPPA statute.[210] Some opined that such a distinction does not take into account how operator-driven personalization can benefit children in educational and other contexts.[211]

By contrast, a coalition of state attorneys general recommended that the Commission amend the definition of support for the internal operations of the website or online service to limit "personalization" to "user-driven" actions.[212] Specifically, the coalition proposed that the Commission limit user-driven personalization to tools that enable users to customize their experience by, for example, configuring layout, content, or system functionality, while excluding personalization that is "based on data collected from what users search, purchase, and watch."[213] The Center for Democracy and Technology also expressed general support for limiting the definition to user-driven rather than operator-driven personalization.[214] This commenter suggested that, if a user signs into his or her account on an app where the user selects an option to see more of a particular type of content or creator, such action should be deemed to be user-driven personalization that falls within the support for the internal operations definition.[215] A few commenters recommended that the Commission restrict the use of the support for the internal operations exception to the COPPA Rule's verifiable parental consent requirement so that it would not be available for user-driven or operator-driven personalization.[216]

---

[209] *See, e.g.*, ACLU, at 21-22.
[210] *See, e.g.*, Chamber, at 5; Privacy for America, at 14.
[211] *See, e.g.*, ESA, at 17; News/Media Alliance, at 3; ANA, at 9.
[212] State Attorneys General Coalition, at 6.
[213] *Id.*
[214] CDT, at 6.
[215] *Id.*
[216] *See, e.g.*, Center for AI and Digital Policy, at 6-7; T. McGhee, at 10.

Some commenters recommended that, if the Commission decides to exclude some personalization techniques from the support for the internal operations of the website or online service definition, the Commission should focus only on personalization that is based upon user profiling[217] or permit personalization in educational products that schools have consented for children to use or that facilitate adaptive learning.[218] Relatedly, an individual commenter opined that operator-driven, profile-based personalization can be beneficial in contexts such as "delivering age-appropriate content, restricting display of adult content, restricting contact by adults, serving content that is relevant to the user, [and] enriching the functionality for a user."[219]

Having carefully considered the record and comments regarding the idea of amending the support for the internal operations of the website or online service definition to exclude operator-driven personalization, the Commission finds persuasive the reasons set forth by commenters that recommended the Commission decline to make such an amendment. The Commission therefore declines to make such an amendment to the definition at this time.[220]

e. NPRM Question Ten: Contextual Advertising

The 2024 NPRM noted that the support for the internal operations exception to the COPPA Rule's verifiable parental consent requirement permits operators to collect persistent identifiers for contextual advertising purposes without parental consent as long as they do not also collect other personal information.[221] Question Ten of the "Questions for the Proposed

[217] *See, e.g.*, ACLU, at 21-22. *See also, e.g.*, Consumer Reports, at 7 (opining that the support for the internal operations exception might properly permit operator-driven personalization for purposes such as preserving a child's progress within a game but should not permit operator-driven personalization to create profiles of children).
[218] *See* Advanced Education Research and Development Fund, at 7.
[219] M. Bleyleben, at 4.
[220] The Commission received relatively little specific response to the portion of Question Nine that asked how operators use persistent identifiers to maximize user engagement. For the reasons set forth in Part II.D.5.c, the Commission is not moving forward with the 2024 NPRM's proposal to prohibit operators from using the support for the internal operations exception to the COPPA Rule's verifiable consent requirement in conjunction with processes that encourage or prompt use of a website or online service.
[221] 89 FR 2034 at 2043.

Revisions to the Rule" section of the NPRM requested comment on whether the Commission should consider changes to the COPPA Rule's treatment of contextual advertising due to the current sophistication of contextual advertising, "including that personal information collected from users may be used to enable companies to target contextual advertising to some extent."[222]

Several commenters responded to Question Ten by expressing concerns with the COPPA Rule's treatment of contextual advertising.[223] Some commenters opined generally that contextual advertising closely resembles targeted advertising by relying upon user-level data and inferences and the use of artificial intelligence.[224] One commenter stated that the COPPA Rule's support for the internal operations exception to the verifiable parental consent requirement does not need to include contextual advertising because persistent identifiers are not needed for contextual advertising, and including within the exception the use of persistent identifiers for contextual advertising "simply opens the door to the sharing of personal information with third parties who do not need it" and "invit[es] leakage into the broader ad ecosystem."[225] Some commenters asserted that contextual advertising allows entities such as data brokers to create and sell profiles.[226] Commenters raising these concerns recommended that the Commission respond by, for example, providing greater clarity as to the meaning of "contextual" advertising, including by narrowing the support for the internal operations exception to permit only contextual advertising that does not vary based on personal information collected from, or related to, the child or by stating explicitly that operators should restrict the personal information

[222] *Id.* at 2070.
[223] *See, e.g.*, Internet Safety Labs, at 5-6; EPIC, at 6-8; M. Bleyleben, at 1, 4-5; State Attorneys General Coalition, at 6-8; Consumer Reports, at 7-8; CDT, at 7; SuperAwesome, at 2-4; T. McGhee, at 11.
[224] *See, e.g.*, EPIC, at 6-8; State Attorneys General Coalition, at 7-8.
[225] M. Bleyleben, at 1. *See also*, *e.g.*, T. McGhee, at 11 (questioning what persistent identifiers are needed for "contextual advertising" about the context and content of the webpage).
[226] *See, e.g.*, Internet Safety Labs, at 5-6.

collected for contextual advertising to what is strictly necessary to deliver contextual advertising.[227]

By contrast, a large number of commenters recommended that the Commission maintain the position that the support for the internal operations exception to the COPPA Rule's verifiable parental consent requirement permits the use of persistent identifiers for contextual advertising.[228] Many such commenters urged that contextual advertising is critical to maintaining free, high quality content for children.[229] Some emphasized that requiring operators to obtain verifiable parental consent to collect and use persistent identifiers for contextual advertising would negatively affect startup and small businesses, in particular.[230] Some commenters emphasized that enabling operators to use contextual advertising is important for ensuring that children do not receive advertising content that is not appropriate for children.[231] Some stated that the COPPA Rule should not require verifiable parental consent for the use of persistent identifiers to serve contextual advertisements because delivering contextual advertisements is a "privacy-centric" advertising practice that does not entail "contacting" a specific individual or child on a one-to-one basis.[232] In addition, a few trade associations

---

[227] *See, e.g.*, EPIC, at 6-8; State Attorney General Coalition, at 5-6; Consumer Reports, at 7-8. *See also, e.g.*, SuperAwesome, at 3-4 (supporting the COPPA Rule permitting operators to collect persistent identifiers for contextual advertising purposes without obtaining parental consent while recommending that the COPPA Rule provide greater clarity as to the distinction between contextual and behavioral advertising).

[228] *See, e.g.*, SIIA, at 6, 17; R Street Institute, at 2-3; ITIC, at 3; 4A's, at 3-4; NAI, at 5-6; Chamber, at 11; NCTA, at 11-13; kidSAFE, at 6-7; ACT | The App Association, at 7; ITIF, at 4; CCIA, at 5-6; The Toy Association, at 4; Google, at 11; Microsoft, at 6; ANA, at 8-10; News/Media Alliance, at 5-6; Privacy for America, at 3-4; IAB, at 20-21; CIPL, at 6; M. Jones, at 1; S. Ward, at 1.

[229] *See, e.g.*, SIIA, at 6, 17; ITIC, at 3; 4A's, at 3-4; Chamber, at 11; IAB, at 20-21; ITIF, at 4; CCIA, at 5-6; Google, at 11; News/Media Alliance, at 5-6; Privacy for America, at 3-4; kidSAFE, at 6-7; NAI, at 5-6; ANA, at 8-10; M. Jones, at 1.

[230] *See, e.g.*, Engine, at 3 (emphasizing that startups rely upon revenue received from contextual advertising); 4A's, at 3-4 (emphasizing that small publishers and content providers rely upon revenue received from contextual advertising).

[231] *See, e.g.*, ITIC, at 3; Microsoft, at 6.

[232] *See, e.g.*, NCTA, at 12 (arguing that contextual ads are by their nature not delivered on a one-to-one basis and thus do not result in "contacting"); News/Media Alliance, at 5 ("Contextual advertising is one of the more privacy-centric advertising practices."). *See also* The Toy Association, at 4 ("[B]y its very nature contextual advertising is

asserted that requiring verifiable parental consent for the use of persistent identifiers to facilitate contextual advertising could violate the Constitution.[233]

Having carefully considered the record and commenters' responses to Question Ten, the Commission declines to modify the COPPA Rule's treatment of contextual advertising. As discussed further in Part II.C.2, the Commission's addition of new section 312.4(d)(3) will enhance the Commission's ability to monitor operators' use of the support for the internal operations exception to the COPPA Rule's verifiable parental consent requirement for contextual advertising and other purposes.

5. Definition of "Website or Online Service Directed to Children"

The Rule's current definition of "web site or online service directed to children" includes in its first paragraph a list of factors that the Commission considers in determining whether a particular website or online service is child-directed. The second paragraph states that 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. The third paragraph provides that certain "mixed audience" websites and online services that are child-directed under the multi-factor test set forth in the first paragraph of the definition will not be deemed directed to children if the website or online service does not collect personal information from any visitor prior to collecting age information and prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under 13 without first complying with the notice and parental consent provisions of the Rule.

---

targeting the audience based on the content they are choosing and making common sense inferences about the audience. For our members[']] experience, AI and machine learning used for contextual advertising only pertains to content analysis of the programming/show where the ads appear and not information collected from the viewer.").

[233] *See, e.g.*, ACT | The App Association, at 7; NCTA, at 12.

The fourth paragraph provides that a website or online service will not be deemed child-directed solely because it refers or links to a commercial website or online service directed to children.

The Commission proposed a number of amendments to this definition in the 2024 NPRM that were intended to provide additional insight and clarity regarding how the Commission currently interprets and applies the definition and were not intended to substantively change the Rule.[234] As explained *infra*, the Commission adopts amendments to paragraphs (1) and (3). The Commission has decided not to make the proposed amendment to paragraph (2) and also declines to adopt an exemption.

a. Paragraph (1) of "Website or Online Service Directed to Children"

i) The Commission's Proposal Regarding Paragraph (1) of "Website or Online Service Directed to Children"

The determination of whether a website or online service is child-directed is fact-based and requires flexibility as individual factors may be more, or less, relevant depending on the context. In the 2024 NPRM, the Commission preserved the multi-factor test for determining child-directedness in the Rule,[235] but proposed amending paragraph (1) of the definition of "website or online service directed to children" to include a non-exhaustive list of examples of evidence the Commission may consider in analyzing audience composition and intended audience. Specifically, the Commission proposed adding to the definition marketing or promotional materials or plans, representations to consumers or to third parties, reviews by users or third parties, and the age of users on similar websites or services.

[234] *See* 89 FR 2034 at 2046.
[235] *See id.* at 2046. The Commission notes that many commenters expressed support for continued application of the multi-factor test. *See, e.*g., ESA, at 2; IAB, at 9; CDT, at 7; CIPL, at 7.

ii) Public Comments Received in Response to the Commission's Proposal Regarding Paragraph (1) of "Website or Online Service Directed to Children"

The Commission received numerous comments in response to this proposal, with many commenters expressing support for including certain proposed examples in the definition of "website or online service directed to children" while opposing the inclusion of other proposed examples.[236]

Regarding the examples of "marketing or promotional materials or plans" and "representations to consumers or to third parties," a majority of commenters addressing the proposal supported including such examples.[237] Some of these commenters emphasized these factors are within operators' control and appropriately focus on the ways that operators signal to consumers, advertisers, and others that children are a targeted audience.[238] For these reasons, the Commission is convinced such materials and representations often provide compelling direct evidence regarding an operator's intended audience and audience composition and notes that complaints in previous COPPA enforcement cases have cited such evidence as being relevant in determining whether a website or online service is directed to children.[239]

Most of the commenters that opposed the Commission's proposal primarily raised concerns with the addition of "reviews by users or third parties" and "the age of users on similar

[236] Certain commenters expressed support for all of the proposed examples. *See, e.g.*, Common Sense Media, at 3; Consumer Reports, at 8; Mental Health America, at 5.
[237] *See, e.g.*, CIPL, at 7; T. McGhee, at 4; NAI, at 6-7; ESRB, at 19; Microsoft, at 8; TechFreedom, at 9-10; News/Media Alliance, at 4; Common Sense Media, at 3; Consumer Reports, at 8; Mental Health America, at 5. Other commenters expressed support for one of these examples. *See* Chamber, at 6 (expressing support for Commission considering marketing and promotional materials in determining child-directedness).
[238] *See* Mental Health America, at 5; NAI, at 6.
[239] *See, e.g.*, Complaint, *United States v. Microsoft Corp.*, Case No. 2:23-cv-00836 (W.D. Wash. June 5, 2023), at 7, available at *https://www.ftc.gov/system/files/ftc_gov/pdf/microsoftcomplaintcivilpenalties.pdf*; Complaint, *FTC v. Google LLC and YouTube, LLC*, Case No. 1:19-cv-02642 (D.D.C. Sept. 4, 2019), at 8-9, 11, 15-16, available at *https://www.ftc.gov/system/files/documents/cases/youtube_complaint.pdf*.

websites or services" to paragraph (1) of the definition. Some commenters contended these examples are not "competent and reliable empirical evidence" of audience composition or intended audience, and are therefore inconsistent with the standard set forth in the final sentence of paragraph (1) and should not be considered in the Commission's assessment of child-directedness.[240] Many commenters also asserted that these examples are subjective or vague,[241] and unlike other factors identified in paragraph (1) of the definition, improperly make operators responsible for factors outside of their knowledge and control.[242] For example, regarding reviews by users or third parties, commenters questioned which reviews the Commission would deem relevant[243] and noted that not all reviews are reliable or genuine.[244] Some commenters also expressed concern that this proposed amendment would incentivize competitors or others to file false reviews in an attempt to influence how a website or online service is categorized.[245]

Regarding the age of users on similar websites or services, commenters emphasized that operators would likely not have access to data about the ages of users of websites or online services controlled by others,[246] and that it is not clear what would be considered a "similar"

[240] *See, e.g.*, IAB, at 9-12 (arguing that user reviews and age demographics of other services are not competent and reliable indicators of child-directedness); NCTA, at 8-9 (arguing the two factors do not meet the heightened standard of competent and reliable empirical evidence); News/Media Alliance, at 4 ("It is our members' experience that reviews by users and third parties are often subjective and tend to be imprecise.").
[241] *See, e.g.*, Chamber, at 6; ESRB, at 19; ESA, at 2-3; NCTA, at 8-9.
[242] *See, e.g.*, CCIA, at 6-7; T. McGhee, at 4; 4A's, at 2; Chamber, at 6; ESA, at 2-3; IAB, at 5-6; NCTA, at 7-8; ACT | The App Association, at 5; ANA, at 7-8; International Center for Law & Economics, at 14-15; Privacy for America, at 5-6; Epic Games, at 11; Google, at 4-5.
[243] *See, e.g.*, American Consumer Institute, at 2; CCIA, at 7; Taxpayers Protection Alliance, at 2. At least one commenter expressed uncertainty about whether the Commission would evaluate user reviews over time, or whether the assessment would be based on evaluating reviews at a particular point of time. *See, e.g.*, ESA, at 3.
[244] *See, e.g.*, CIPL, at 7; ANA, at 7.
[245] *See, e.g.*, ANA, at 7 ("[L]isting reviews as a factor in this test incentivizes competitors to file false reviews in an attempt to influence how a website or online service is categorized."); TechFreedom, at 11-12 ("allowing third-party reviews to color the intent of the website or service provider almost guarantees the weaponization of this new definition").
[246] *See, e.g.*, American Consumer Institute, at 2; ANA, at 8; CCIA, at 7; Google, at 4-5.

website or service.[247] Many industry commenters also emphasized that monitoring third-party reviews or gathering available information about the age of users of "similar" websites and online services would significantly increase operators' compliance burdens.[248] Others suggested that inclusion of such evidence in the definition would be inconsistent with the Commission's position that operators of general audience properties have no duty to investigate the ages of visitors to their properties under COPPA[249] and would inappropriately import a constructive knowledge standard into the Rule that is inconsistent with the COPPA statute.[250]

In response to these comments, the Commission reiterates that the inquiry in determining child-directedness requires consideration of a totality of the circumstances. Depending on the facts, reviews or the age of users on similar websites or online services may receive little weight in determining audience composition or the intended audience of a website or online service. For example, the Commission understands that reviews may not always be representative, accurate, or genuine and that content ratings or other ratings published by platforms or other third parties are developed for a range of different purposes that are not necessarily fully aligned with determining whether a website or online service is directed to children under the COPPA Rule.[251] The Commission will take such considerations into account when determining whether to rely on such evidence in assessing child-directedness. The Commission also observes that it is common for companies to monitor reviews related to their websites or online services as well as

[247] *See, e.g.*, ANA, at 8; CCIA, at 6-7; International Center for Law & Economics, at 14-15; Privacy for America, at 5-6; Google, at 4-5; NetChoice, at 4; Taxpayers Protection Alliance, at 2; News/Media Alliance, at 4-5; ESA, at 3; CIPL, at 7.
[248] *See, e.g.*, Privacy for America, at 6; CCIA, at 7; 4A's, at 2; ANA, at 7-8. Some such commenters asserted that such monitoring may be "entirely infeasible" for small operators. Privacy for America, at 6; 4A's, at 2.
[249] *See* Privacy for America, at 5-6; ACT | The App Association, at 5.
[250] *See, e.g.*, SIIA, at 18; IAB, at 10-11.
[251] *See, e.g.*, ESRB, at 20 (suggesting reviews by third parties could potentially include content ratings which would be inappropriate for the Commission to consider because such ratings are about the appropriateness of content rather than whether a service is directed to children).

to track information about user demographics and the features of competitors' websites or online services. The addition of these examples to the definition of "website or online service directed to children" is not intended to impose a burdensome requirement that operators identify and continuously monitor all such information. However, there certainly may be circumstances in which operators' knowledge of reviews or the ages of users on similar websites or services may be relevant to the Commission's determination, based on the totality of the circumstances, that a website or service is directed to children.[252]

iii) The Commission Amends Paragraph (1) of "Website or Online Service Directed to Children"

After carefully considering the record and comments, and for the reasons discussed in Part II.B.5.a.ii of this document, the Commission has decided to amend paragraph (1) of the definition as proposed.

b. NPRM Question Eleven: Potential Exemption from "Website or Online Service Directed to Children"

In Question Eleven of the "Questions for the Proposed Revisions to the Rule" section of the NPRM, the Commission requested comment on various questions related to whether it should offer an exemption within the definition of website or online service directed to children, or other incentive, if an operator of a website or online service undertakes an analysis of its

[252] If an operator is aware of publicly-available information indicating that children under 13 are using its website or online service, such information may be relevant to determining that the website or online service is child-directed. For example, in a complaint against Epic Games, the Commission alleged the company and its employees also regularly monitored, read, and circulated news articles and social media posts chronicling Fortnite's popularity among children, and sometimes incorporated kids' ideas directly into the game. *See* Complaint, *United States v. Epic Games, Inc*., Case No. 5:22-CV-00518 (E.D.N.C. Dec. 19, 2022), at 15, available at *https://www.ftc.gov/system/files/ftc_gov/pdf/2223087EpicGamesComplaint.pdf*. In an enforcement case involving a weight-loss app directed to children, the Commission's complaint highlighted that defendants featured consumer reviews from young children to market their app in the Apple App Store. Complaint, *United States v. Kurbo, Inc. and WW International, Inc.*, Case No. 22-cv-946 (N.D. Cal. Feb. 16, 2022), at 7, available at *https://www.ftc.gov/system/files/ftc_gov/pdf/filed_complaint.pdf*.

audience composition and determines that no more than a specific percentage of its users are likely to be children under 13.[253]

The Commission received some comments supporting such an exemption.[254] One FTC-approved COPPA Safe Harbor program suggested an exemption would motivate operators to thoroughly investigate their audiences without fear of collecting evidence that might be used in government enforcement actions.[255] An industry commenter suggested an exemption would allow operators of sites with a small percentage of users under 13 to avoid unnecessary compliance costs and better tailor their services to their audience, and provide the FTC with greater insight into online services' audiences.[256]

However, a large majority of commenters addressing Question Eleven opposed implementing such an exemption.[257] Commenters opposing or expressing skepticism about this potential exemption raised concerns such as the possibility of operators manipulating data,[258] difficulties in handling fluctuations in user bases over time,[259] and doubts about the efficacy of methods used to determine age.[260] Several commenters argued that incentivizing audience analysis with an exemption would increase the collection of personal data and reduce privacy for

---

[253] *See* 89 FR 2034 at 2070 (Question 11). Question Eleven's subsidiary questions included what are reliable means by which operators can determine the likely ages of their sites' or services' users (Question 11(b)) and whether inclusion of an audience composition-based exemption within the definition of "website or online service directed to children" would be inconsistent with the COPPA Rule's multi-factor test for determining whether a website or online service, or a portion thereof, is directed to children (Question 11(e)).
[254] *See, e.g.*, CARU, at 2; ITIF, at 4. *See also generally* Family Online Safety Institute, at 3-4 (responding to Question Eleven by expressing the view that age assurance processes can improve online safety for young users by enabling operators to offer age appropriate online experiences).
[255] CARU, at 2. However, another FTC-approved COPPA Safe Harbor program saw limited value in the proposal. *See* kidSAFE, at 7-8.
[256] ITIF, at 4-5.
[257] *See, e.g.*, Motley Rice, at 8-10; IAB, at 15-16; NCTA, at 9-10; Center for AI and Digital Policy, at 8-9; State Attorneys General Coalition, at 8-9; A. Artman, at 2; M. Bleyleben, at 6; The Toy Association, at 5. *See also, e.g.*, Consumer Reports, at 8-9 (cautioning against any incentive that would lead operators to collect additional data on consumers); T. McGhee, at 11-12 (asserting that such an incentive could be better handled in a controlled environment such as under the supervision of FTC-approved COPPA Safe Harbor programs).
[258] *See, e.g.*, Motley Rice, at 8-10.
[259] *See, e.g.*, T. McGhee, at 11-12; IAB, at 15-16.
[260] *See, e.g.*, Center for AI and Digital Policy, at 8-9; IAB, at 14-15.

all visitors.[261] A significant number of commenters viewed the approach as being inconsistent with the multi-factor approach that is central to determining whether a website or online service is directed to children.[262] One industry commenter argued that it would be potentially inconsistent with the COPPA statute to treat the number of child visitors to a website or online service as the "sole determinative factor" in determining whether a website or online service is child-directed and that other factors such as the intent of the operator and whether content is child-directed are more relevant factors.[263] Another industry commenter suggested incentivizing age estimation and the collection of additional information from website visitors could unconstitutionally restrict access to speech, encourage unreliable age analysis techniques, perpetuate bias if age estimation techniques rely on information from photographs or user behavior, and would disadvantage, and be unduly burdensome for, small and medium-sized businesses with fewer resources to conduct sophisticated age analyses.[264]

After carefully considering the record and comments, the Commission has determined not to move forward with an exemption related to audience analysis at this time. The Commission is persuaded by the comments suggesting that an exemption based on audience composition may be inconsistent with the multi-factor approach used to determine whether a website or online service is child-directed as well as the comment suggesting that small and medium-sized businesses may be disadvantaged by such a provision because they have fewer resources to conduct and update audience analyses.

[261] *See, e.g.*, ESA, at 4; State Attorneys General Coalition, at 9; CDT, at 7-8; Consumer Reports, at 8; IAB, at 13.
[262] *See, e.g.*, IAB, at 13; NCTA, at 9-10; CIPL, at 2; Center for AI and Digital Policy, at 9. *See also* M. Bleyleben, at 5 (expressing view that the multi-factor test has been effective and opposing audience composition exemption).
[263] The Toy Association, at 5.
[264] IAB, at 13-15.

c. Paragraph (2) of "Website or Online Service Directed to Children"

i) The Commission's Proposal Regarding Paragraph (2) of "Website or Online Service Directed to Children"

Currently, the second paragraph of the definition of "[w]eb site or online service directed to children" states that "[a] Web site 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 Web site or online service directed to children."[265] In the 2024 NPRM, the Commission explained this provision was added to the Rule as part of the 2013 Amendments, along with certain changes to the definition of operator, to clarify that the operator of a child-directed website or online service is strictly liable when a third party collects personal information through its website or online service, while the third party is liable under COPPA only if it had actual knowledge that the website or online service from which it was collecting personal information was child-directed.[266] The Commission proposed removing the term "directly" from paragraph (2) in the 2024 NPRM to address the possibility that third parties could knowingly receive 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.[267]

ii) Public Comments Received in Response to the Commission's Proposal Regarding Paragraph (2) of "Website or Online Service Directed to Children"

[265] 16 CFR 312.2.
[266] 89 FR 2034 at 2047.
[267] *See id.*

Commenters supporting the proposal agreed that the amendment addressed a "loophole" that is contrary to COPPA's intent.[268] Some of these commenters argued that adopting the proposal would help ensure that advertising networks do not get access to children's personal information without first obtaining verifiable parental consent.[269]

However, a majority of the commenters addressing this proposal opposed it, raising several concerns.[270] Some commenters raised practical issues with extending COPPA obligations to downstream third parties, such as difficulties facing third parties in determining whether the first party properly collected information in compliance with COPPA[271] and how third parties could satisfy COPPA's notice and consent requirements without a direct relationship to the child or parents.[272] Other commenters argued that the removal of "directly" departs from express limitations in the COPPA statute.[273] For example, some commenters contended "actual knowledge" triggers COPPA's requirements under 15 U.S.C. 6502(a)(1) only where the operator knows that it is collecting personal information "from a child" and does not extend to a third party's actual knowledge of another service's child-directedness when the third party is not collecting personal information directly from the child.[274] Commenters contended the proposed amendment would expand the scope of covered operators beyond what is specified in the COPPA statute and would be inconsistent with Congress' intent when enacting the COPPA

[268] Children and Screens, at 4. *See also* SuperAwesome, at 1-2 (supporting proposal of removing "directly" to cover ad exchanges and ad networks); Common Sense Media, at 9-10 (supporting proposal "to ensure that operators who are ad networks who are integrated with children directed content, or on sites with known child users and who collect information from users of those sites, are liable even if information collection is not 'directly from children'").
[269] Common Sense Media, at 9.
[270] *See, e.g.*, Chamber, at 7; IAB, at 24-25; CIPL, at 7-8; ACLU, at 5-7; ANA, at 11.
[271] *See, e.g.*, IAB, at 25 (proposal would "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 exceeds the bounds of the statute ….").
[272] *See, e.g.*, CIPL, at 7-8; IAB, at 25.
[273] *See, e.g.*, IAB, at 24-25; CIPL, at 7-8; ACLU, at 5-7; ANA, at 11.
[274] *See, e.g.*, IAB, at 24-25 ("The proposed definition would improperly render superfluous the statutory requirement that collection be 'from a child.'").

statute.[275] One public interest group commenter argued the Commission's proposal to regulate third parties that are indirectly collecting personal information from children raises First Amendment concerns because it restricts third parties' receipt and possession of information.[276]

iii) The Commission Declines to Amend Paragraph (2) of "Website or Online Service Directed to Children"

Given the general lack of support for the NPRM proposal, the Commission has decided not to remove the term "directly" from paragraph (2) of the definition of "website or online service directed to children." Practical considerations, such as how a third party would provide notice and obtain verifiable parental consent in accordance with the COPPA Rule without having a direct relationship to the child or parent, make the proposal difficult to implement. In addition, given other proposed amendments the Commission is finalizing,[277] the Commission believes that this proposed amendment is not necessary to protect the privacy of personal information collected from children. Specifically, because the Rule amendments the Commission is finalizing clarify that operators must obtain separate verifiable parental consent for disclosures to third parties, parents will have to provide consent for disclosures to third parties such as ad networks.

---

[275] *See, e.*g., ANA, at 11 ("This change would expand COPPA compliance burdens, as well as COPPA enforcement and fines, to a large universe of entities previously not subject to the law, merely on the basis of being 'downstream' data recipients."); NetChoice, at 4 (suggesting proposal "would sweep in many more websites and online services, even those not targeting children as their primary audience, imposing COPPA obligations on them and restricting general audience content"); IAB, at 24-25 (contending proposed change "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."). Commenters raised additional concerns with this proposal, such as that it would impose substantial burdens on third parties to assess and reassess the COPPA status of all vendors they receive data from. *See* Chamber, at 7 ("Removing the direct collection requirement would [] create further uncertainty, particularly if no determination has been made by the Commission or the third-party that a third-party website's content is directed to children."); IAB, at 25 (suggesting proposed change "would, in effect, require a recipient of personal information to assess the COPPA status of all vendors from which it receives data" and that "[c]ompliance would become particularly difficult when vendors rebrand or launch new products or services that could change their status under COPPA.").

[276] ACLU, at 6-7.

[277] *See* Part II.D.1 discussing § 312.5(a)(2) of the Rule.

The Commission also notes that in circumstances where downstream entities receive personal information collected from children on a child-directed website or online service, the operator of the child-directed site or service and any third party that has actual knowledge that it is collecting personal information directly from users of another website or online service that is directed to children would be liable for violating COPPA.[278] The operator and entities that collect directly from the operator's users on behalf of the operator thus have powerful incentive not to allow downstream entities to violate COPPA. Also, many operators and companies in the advertising ecosystem transmit COPPA flags or signals indicating that the personal information or other traffic sent with the flag or signal is associated with a child. Companies that receive these signals are directly liable under COPPA on the basis that they have actual knowledge that the individual user is a child, regardless of whether they collected information from the child-directed site directly.

d. Proposed Amendment to Paragraph (3) of "Website or Online Service Directed to Children"

In the 2024 NPRM, the Commission proposed amending paragraph (3) of the definition of "website or online service directed to children" to remove content now covered by the new proposed definition for "mixed audience website or online service" and adding a statement clarifying that "[a] mixed audience website or online service shall not be deemed directed to children with regard to any visitor not identified as under 13."[279] No comments were received addressing this specific proposed amendment of paragraph (3). For the reasons discussed in Part II.B.1, the Commission has decided to adopt a new stand-alone definition for "mixed audience

[278] *See, e.g.*, Office of the New York State Attorney General, *A.G. Underwood Announces Record COPPA Settlement with Oath – Formerly AOL – For Violating Children's Privac*y, available at *https://ag.ny.gov/press-release/2018/ag-underwood-announces-record-coppa-settlement-oath-formerly-aol-violating*.
[279] 89 FR 2034 at 2047-2048, 2072.

website or online service" and is accordingly amending paragraph (3) of the definition of "website or online service directed to children" as proposed.

C. Section 312.4: Notice

1. Section 312.4(c): Content of the Direct Notice

In the 2024 NPRM, the Commission proposed various amendments to § 312.4(c) of the COPPA Rule, which governs "[c]ontent of the direct notice to the parent." In totality, the proposed amendments would expand the disclosures required in direct notices.

As a threshold matter, one commenter generally opposed expanding the disclosures required in direct notices, warning that such expansion "will add regulatory burden without creating any added privacy or benefits for children or consumers generally."[280] The Commission disagrees. As multiple other commenters asserted,[281] the proposed amendments to the direct notice requirements will empower parents to make informed choices when navigating online services with children and clarify operators' obligations under this section of the Rule.

a. Proposals Related to § 312.4(c)(1), 312.4(c)(1)(i), 312.4(c)(1)(ii), and 312.4(c)(1)(vi)

i) The Commission's Proposals Regarding § 312.4(c)(1), 312.4(c)(1)(i), 312.4(c)(1)(ii), and 312.4(c)(1)(vi)

Under the current Rule, § 312.4(c)(1) sets forth the required content of the direct notice when an operator collects personal information in order to initiate a request for parental consent under the parental consent exception set forth in § 312.5(c)(1).[282]

[280] NCTA, at 16.
[281] *See, e.g.*, Children's Advocates Coalition, at 39-40; Consumer Reports, at 9.
[282] *See* 16 CFR 312.4(c)(1).

In the 2024 NPRM, the Commission proposed amending the heading of § 312.4(c)(1) and making minor amendments to § 312.4(c)(1)(i), (ii), and (vi).[283] Specifically, the Commission proposed adding after "[c]ontent of the direct notice to the parent" in the heading of § 312.4(c)(1) the phrase "for purposes of obtaining consent, including . . . ."[284] This proposed amendment was intended to 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.[285] The Commission also proposed amending § 312.4(c)(1)(i), which currently requires, in relevant part, that the direct notice state "[t]hat the operator has collected the parent's online contact information from the child…." The Commission proposed adding "If applicable" to the beginning of this paragraph, and to include "or child's" online contact information in addition to the parent's, to align with the related verifiable parental consent exception in § 312.5(c)(1).[286] The next paragraph, § 312.4(c)(1)(ii), requires the direct notice to state that "the parent's consent is required for the collection, use or disclosure of such information." The Commission proposed replacing "such" with "personal" to clarify that this paragraph refers to the collection, use, or disclosure of personal information.[287] Finally, the Commission proposed amending what is currently § 312.4(c)(1)(vi) (proposed to be redesignated as § 312.4(c)(1)(vii)). That paragraph currently states that operators must also explain in the direct notice that "if the parent does not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the parent's online contact information from its records." For clarity, the Commission proposed adding, "If the operator has collected the name or online contact information of the

[283] As discussed in Part I.A., the Commission is not finalizing at this time the 2024 NPRM's proposals related to school authorization. Consequently, the Commission is neither finalizing the proposed changes to § 312.4(b) nor deleting the phrase "to the parent" in the heading for § 312.4(c).
[284] 89 FR 2034 at 2049.
[285] *Id.* at 2049.
[286] *Id.* at 2049.
[287] *Id.*

parent or child to provide notice and obtain parental consent," to the beginning of this paragraph, inserting "or child's" before "online contact information," and adding "and the parent's or child's name" before "from its records."[288]

ii) Public Comments Received in Response to the Commission's Proposals Regarding § 312.4(c)(1), 312.4(c)(1)(i), 312.4(c)(1)(ii), and 312.4(c)(1)(vi)

The Commission received minimal feedback about these proposals. Without specifically supporting or opposing the proposed amendment, CIPL suggested that the proposed change to the § 312.4(c)(1) heading "greatly expands the scope of" § 312.4(c)(1) because it clarifies that § 312.4(c)(1)'s requirements apply to all instances in which an operator provides direct notice to a parent for purposes of obtaining consent rather than applying only when an operator is collecting a parent's online contact information pursuant to the parental consent exception provided by § 312.5(c)(1) of the Rule.[289] The Commission proposed revising the § 312.4(c)(1) heading because the Commission is aware that, in some contexts, operators may initiate the process of seeking parental consent by means that do not require collecting online contact information.[290] The proposed revision to the heading makes clear that the direct notice requirements set forth in § 312.4(c)(1) applies whenever an operator is seeking verifiable

[288] Because the Commission proposed to add a new paragraph (c)(1)(iv) requiring that direct notices to parents contain information concerning disclosures of personal information to third parties, the Commission also proposed redesignating § 312.4(c)(1)(iv), (v), and (vi) as paragraphs (c)(1)(v), (vi), and (vii), respectively. *See* 89 FR 2034 at 2073. The Commission did not receive any comments concerning the proposals to redesignate these paragraphs and therefore adopts those proposals without change.
[289] CIPL, at 9.
[290] For example, in the 2024 NPRM, the Commission highlighted that an operator could use an in-app pop-up message that directs a child to hand a device to the parent and then instructs the parent to call a toll-free number. 89 FR 2034 at 2049.

parental consent from a parent.[291] The Commission did not receive comments relating to the other proposed amendments to § 312.4(c)(1)(i), (ii), and (vi).

iii) The Commission Amends § 312.4(c)(1), 312.4(c)(1)(i), 312.4(c)(1)(ii), and 312.4(c)(1)(vi)

After careful consideration of the record and comments, and for the reasons discussed above, the Commission has concluded that the proposed amendments clarify operators' obligations and appropriately extend the requirements of § 312.4(c)(1) to all instances in which the operator provides direct notice to a parent for the purposes of obtaining consent. The Commission therefore adopts the proposed amendment to the heading of § 312.4(c)(1) and the other proposed amendments to paragraphs 312.4(c)(1)(i), (ii), and (vi) (redesignated as § 312.4(c)(1)(vii)) as originally proposed.

b. Proposal Related to § 312.4(c)(1)(iii)

i) The Commission's Proposal Regarding § 312.4(c)(1)(iii)

Section 312.4(c)(1)(iii) currently requires the direct notice to include "[t]he additional items of personal information the operator intends to collect from the child, or the potential opportunities for the disclosure of personal information, should the parent provide consent." In the 2024 NPRM, the Commission proposed to amend § 312.4(c)(1)(iii) by deleting "additional," inserting a requirement for the direct notice to state "how the operator intends to use such information," and replacing "or" with "and."[292]

ii) Public Comments Received in Response to the Commission's Proposal Regarding § 312.4(c)(1)(iii)

[291] *See* 89 FR 2034 at 2049 (explaining that the amendment is intended to clarify that the operator must provide the relevant aspects of the 312.4(c)(1) direct notice to the parent even where the operator does not collect personal information to initiate consent under 312.5(c)(1)).
[292] 89 FR 2034 at 2049.

Several commenters generally supported the proposed requirement for the direct notice to state how the operator intends to use the personal information collected from the child if the parent provides consent. The Center for Democracy and Technology, for example, stated that "[a]dditional information about the intended use of the child's data is vital for ensuring the parent gives fully informed consent for the operator to collect their child's data, and therefore should be included in the [direct] notice."[293] And a coalition of state attorneys general similarly stated that the proposed requirement "represents a significant step toward enhancing parental understanding and decision-making regarding consent to their child's personal information collection."[294]

Some commenters that supported these additions also suggested the Commission take further steps to "provide parents with a more comprehensive understanding of how their child's data may be utilized beyond the initial collection, enabling them to make more informed decisions regarding consent."[295] A children's advocates coalition supported the proposed requirement but also proposed that the Commission add "more clarity" by requiring that the direct notice "t[ie] each personal data element or categories of personal data to a stated purpose."[296] Similarly, the state attorneys general coalition encouraged the Commission to require operators "to disclose the purpose or use for each item of information if it's intended to be shared with a third party."[297]

The Commission agrees with the children's advocates coalition and the state attorneys general coalition that, in some instances, direct notices disclosing how the operator would use

[293] CDT, at 3.
[294] State Attorneys General Coalition, at 17.
[295] *Id.*
[296] Children's Advocates Coalition, at 39.
[297] State Attorneys General Coalition, at 17-18 (recommending "[f]or instance, if an operator plans to collect a child's first name, geolocation, and address, they should be obligated to disclose the specific purpose for why the name, geolocation, and address, individually, will be shared with third parties").

each element of personal information the operator collects would be most helpful to parents. In other instances, however, the Commission is concerned that an item-by-item correlation of personal information elements and uses could be superfluous, unduly complex, and in tension with the need for direct notices to be clear and concise.

iii) The Commission Amends § 312.4(c)(1)(iii)

After careful consideration of the record and comments, and for the reasons discussed in Part II.C.1.b.ii, the Commission believes the amendments the Commission proposed to § 312.4(c)(1)(iii) would further the important goals of increasing operator transparency and empowering parents. The Commission is therefore finalizing the amendments to § 312.4(c)(1)(iii) as originally proposed.

c. New § 312.4(c)(1)(iv) Regarding Disclosure of Sharing of Personal Information with Third Parties

i) The Commission's Proposal Regarding New § 312.4(c)(1)(iv)

In the 2024 NPRM, the Commission proposed adding new § 312.4(c)(1)(iv)[298] to require that operators sharing personal information with third parties (including the public if making personal information publicly available) identify in the direct notice to parents for purposes of obtaining consent the third parties as well as the purposes for such sharing, should the parent provide consent.[299] Proposed § 312.4(c)(1)(iv) would also require the operator to state that the parent can consent to the collection and use of the child's information without consenting to the

[298] The Commission also proposed redesignating § 312.4(c)(1)(iv), (v), and (vi) as paragraphs (c)(1)(v), (vi), and (vii), respectively. *See supra* note 288.
[299] *See* 89 FR 2034 at 2049.

disclosure of such information, except to the extent such disclosure is integral to the nature of the website or online service.[300]

ii) Public Comments Received in Response to the Commission's Proposal Regarding New § 312.4(c)(1)(iv)

Many commenters addressed whether proposed new § 312.4(c)(1)(iv) should require operators to identify in the direct notice by name or by category the third parties to which disclosures would be made. In separate comments, Common Sense Media and a children's advocates coalition each urged the Commission to require operators to identify third parties by name *and* category, stating that doing so was necessary to ensure parents' decision-making was adequately informed.[301] As Common Sense Media observed, many parents may not be familiar with the names of third-party, business-to-business service providers that have little or no consumer-facing presence, so categorization of such third parties by the operator could shift the burden of identification away from busy parents.[302] The children's advocates coalition similarly asserted that identification by name and category is necessary to "allow[] parents and advocates to evaluate an operator's practices for personal comfort and legal compliance."[303] The children's advocates coalition further advised the FTC to "prescribe categories itself" to prevent operators from "us[ing] meaningless terms or non-specific examples to disguise their practices."[304]

Other commenters argued that operators should only be required to identify the categories of third parties to which disclosures would be made.[305] One such commenter noted that "the

[300] *See id.*
[301] *See* Common Sense Media, at 8; Children's Advocates Coalition, at 41.
[302] *See* Common Sense Media, at 8.
[303] Children's Advocates Coalition, at 41.
[304] *Id.* (stating that operators' current practices are inconsistent, using "phrases [that] do not have clear or generally-accepted definitions" and "[v]ague terms like 'affiliates' [that] thwart a parent's ability to fully assess the operator's notice and give their consent").
[305] *See, e.g.*, Epic Games, at 6; CCIA, at 7; CIPL, at 9-10.

identities of third parties may be subject to frequent change" for some businesses, which would make disclosing the identities of such third parties challenging for these businesses.[306] Another commenter opined that naming individual recipients in the direct notice would be "impractical" since the direct notice "is intended to be brief and approachable."[307]

Two commenters from the advertising industry—the American Association of Advertising Agencies and Privacy for America—opined that operators should not be required to identify the names or categories of third-party disclosure recipients at all.[308] These commenters asserted that any such requirement would lead to long notices that do not "advance accountability or meaningful transparency."[309] Privacy for America further asserted that requiring operators to identify the names or categories of third-party disclosure recipients would chill competition for service providers and "increase the risk of anticompetitive behavior" by forcing operators to "reveal sensitive commercial information about themselves and their partners."[310]

---

[306] CIPL, at 9-10.

[307] ACLU, at 19-20 (emphasizing, however, that "[a]lthough the brevity of the direct notice may limit the practicality of listing each individual recipient of a child's personal information, parents should still have access to that information" and suggesting the Commission amend § 312.3(c) to require operators to "[p]rovide a reasonable means for a parent to review . . .the specific personal information disclosed to third parties and the identi[t]y of each individual recipient").

[308] *See* 4A's, at 4 ("These requirements will lengthen and complicate privacy notices for parents to review and create competition concerns among operators. While notice, transparency, accountability, and consumer choice are values that 4A's members hold in efforts to protect children's privacy, any proposed changes to COPPA notices must balance the value of the disclosure with consumer benefits, operational realities, and the need for a competitive advertising marketplace."); Privacy for America, at 9 ("Setting forth the identities or specific categories of third parties and purposes of disclosure to such parties in the direct notice to parents will harm competition and lead to confusing notices.").

[309] Privacy for America, at 9-10. *See also* 4A's, at 4.

[310] Privacy for America, at 10 (arguing that "operators likely would be incentivized to list all potential third parties, or categories of third parties, and all potential purposes for disclosures to avoid the possible need to notify parents and obtain new consent if the operator's practices changed," and "[t]he Commission's proposal would also harm innovation and competition" by exerting a "chilling effect on competition among service providers," incentivizing operators "to work with only large vendors that can provide a variety of services," and "reveal[ing] sensitive commercial information about themselves and their partners").

The Commission agrees with the commenters that suggested knowing the third parties with which an operator shares children's personal information is an important consideration for parents. The Commission believes that requiring operators to identify such third parties in the direct notice will enhance parents' ability to make an informed decision about whether to consent to the collection of their child's personal information. The Commission also agrees with the many commenters that stressed the importance of clear and concise direct notices. Accordingly, the Commission believes the Rule should provide operators with enough flexibility to ensure they are able to meaningfully identify the third-party disclosure recipients in a direct notice that is also clear and concise. In some cases, the Commission believes that categories may help parents understand the implications of the parent's decision in a way that names may not, particularly where the third party might be unfamiliar to consumers (*e.g.*, because the third party has little or no consumer-facing presence).[311] In other cases, for example where an operator discloses children's personal information to a small set of well-known third parties, identifying third parties by name may be more informative and more efficient than identifying third parties by category.[312]

Many commenters also weighed in with views on where operators should be required to identify the third parties to which disclosures would be made.[313] Citing the likely importance of the information to parents, and the different purposes served by the different notices, several

[311] Of course the categories that operators use to identify third-party disclosure recipients cannot themselves be deceptive. They must be meaningful and specific.
[312] Where an operator changes the roster of third-party recipients to which it discloses children's personal information after the operator has provided the roster of such recipients in its online notice, the Commission is not likely to consider the addition of a new third party to the already-disclosed category of third-party recipients to be a material change that requires new consent *See, e.g.*, 64 FR 59888 at 59895 ("Thus, for example, if the operator plans to disclose the child's personal information to a new operator with different information practices than those disclosed in the original notice, then a new consent would be required"); *see also id.* at n.107.
[313] Question Twelve in the "Questions for the Proposed Revisions to the Rule" section of the 2024 NPRM requested that commenters address whether it would be better for the COPPA Rule to require operators that share personal information with third parties to identify the third parties by name or category in the operators' direct notices to parents required under § 312.4(c) or their online notices required under § 312.4(d). 89 FR 2034 at 2070.

commenters urged the FTC to require operators to identify such third parties both in the direct notice required under § 312.4(c) and the online notice required under § 312.4(d),[314] as the Commission proposed in the 2024 NPRM.[315] Other commenters worried that direct notices would become unduly long and complex if third parties must be identified in the direct notice, and recommended the FTC only require operators to identify the third parties to which disclosures would be made in the online notice.[316] Balancing the importance of the information

[314] *See, e.g.*, Children and Screens, at 4 ("When operators share personal information with third parties, they should be required to identify those third parties or specific categories of those third parties in the direct notice to the parent, and in the online notice."); Internet Safety Labs, at 8 ("Why is this an either/or and not a 'both'? It must be included in the direct notice under section 312.4(c) for the parent to provide initial consent. This notice is likely to be processed by the parent at the time of provisioning the service for the child. Whereas the notice in 312.4(d) is likely to be accessed while the service is used. Thus, if the third-party sharing behavior changes, it is more likely to be observed/noticed in the online notice."); Children's Advocates Coalition, at 42 ("[W]e urge the Commission to require such identification in both the direct and online notices."); EPIC, at 8 ("This information must be included in both the direct notice to parents as well as notice posted on the website."); Consumer Reports, at 9 ("The third parties with which a operator shares personal data is likely one of the key decision points upon which parents evaluate their consent choices (for example, whether the operator shares personal data with social media companies or data brokers) and thus this type of information should be shared up-front in the direct notice, as well as in the online notice required under § 312.4(d)."); M. Bleyleben, at 5 ("Why not both? It's hard enough to ensure parents get the information they need. They should get it both proactively (direct notice) and if they click through to it from the site or search for it on the service itself (online notice).").

[315] The Commission proposed changing the Rule to require that operators provide the identities or specific categories of any third-party disclosure recipients in the direct notice and the online notice, and sought comment on whether such information was better positioned in the direct notice or the online notice. *See* 89 FR 2034 at 2049-2050, 2070.

[316] *See, e.g.*, CARU, at 4 ("CARU believes that, because the identity or category list may be long, it might detract from other more important information required in the direct notice to parents; therefore, it is most appropriately placed in the online notice required under § 312.4(d)."); kidSAFE, at 8 ("While kidSAFE generally supports the FTC's clarification of the notice requirements under this exception, we urge the FTC not to require lengthier and more complex direct notice statements. Information about data usage practices and the identities or categories of third parties with whom personal information may be shared should not be required within direct notices and is better suited for the fuller privacy policy."); Engine, at 2 ("Many of the third parties in a startup[']s technology stack are unlikely to be familiar to parents, like content delivery networks or software development kits, etc. In the interest of maintaining clear and concise direct notices that both ease burdens on startups and place parents' attention on truly important disclosures, this information should be relayed in the online notice."); J. Chanenson et al., at 1-2 ("[I]t would be more advantageous for privacy researchers and parents alike to have the information posted within the online notice [] rather than the direct notice []. Placing details about third-party sharing in the online notice offers several benefits. Firstly, an online platform provides a centralized and easily accessible location for comprehensive information, allowing researchers and parents to efficiently analyze and compare privacy practices across multiple operators. . . . Furthermore, requir[ing] third-party disclosure in the online notice enhances the longevity and accessibility of the information, ensuring that researchers can reference and track changes over time."); The Toy Association, at 7 ("We also question the utility of requiring that operators that share personal information with third parties identify those third parties, or specific categories of those third parties, in the direct notice to parents. Direct notices to parents must contain certain specific information and a link to the posted privacy policy. This allows notices to be reasonably succinct and provides the vehicle for them to access additional information. Several state laws . . . already require disclosing categories of third-party recipients in posted privacy

to parents with the utility of clear and concise direct notices, some commenters suggested a hybrid or "nested" information approach, recommending that operators be required to include hyperlinked cross-references in their direct and online notices.[317]

Considering the likely importance of the information to parents, and the role that direct notices play in helping parents make informed decisions, the Commission agrees with those commentators that urged the Commission to require operators to identify third-party disclosure recipients in the direct notice (as well as the online notice). To mitigate concerns that such a requirement might lead to unduly long and complex direct notices, and mindful of the different contexts in which parents may encounter the different notices, the Commission notes that operators may include a hyperlinked cross-reference from the direct notice to the section in the operator's online notice where operators are able to provide more detail regarding the third parties to which, and the purposes for which, the operator discloses personal information.

In addition to whether operators must identify third-party disclosure recipients by name or category, and whether operators must include such identification in operators' direct and online notices, commenters also addressed other aspects of proposed § 312.4(c)(1)(iv). Some commenters emphasized that operators should be required to state which disclosures are integral to the nature of the website or online service,[318] reasoning, for example, that such delineation would serve as "a crucial layer of protection" to prevent parents from "unwittingly providing consent to a broader range of disclosures than they may have intended."[319] As a children's advocates coalition put it, "[t]he consent request should clearly state which personal information

policies, so placing this information in the direct notice would be redundant. These proposed requirements will simply make notices longer and more cumbersome, will be difficult to read (especially in text message form), and are unlikely to be meaningful to parents.").

[317] *See, e.g.*, M. Bleyleben, at 5; SIIA, at 18; Google, at 7; T. McGhee, at 13.

[318] *See, e.g.*, J. Chanenson et al., at 3; Center for AI and Digital Policy, at 10. As discussed in Part II.C.1.c.iii of this document, the Commission is not including the words "the nature of" in § 312.4(c)(1)(iv) of the Rule.

[319] J. Chanenson et al., at 3.

element or which category of personal information will be shared with which third party and for what purpose,"[320] and "the Commission should clarify that data shared for a particular purpose can only be used for that specified purpose and must not be used for any other purposes."[321] Moreover, where the subject website or online service facilitates public disclosure of a child's information, the children's advocates coalition further argued that operators should have a "heightened responsibility to alert parents to the risks" of such disclosure.[322] One commenter, however, expressed concern that "requiring the disclosure of business practices necessary to ensure compliance with a law would [] likely expose sensitive, nonpublic business information."[323]

Under proposed § 312.4(c)(1)(iv), and the proposed amendments to § 312.4(c)(1)(iii), operators would be required to provide direct notices that clearly state (by name or category) which third parties[324] would receive personal information for what purpose—including the public if a child's personal information would be made publicly available. Accordingly, the use of a child's personal information by a third party for an undisclosed purpose would violate the Rule. Further, because proposed § 312.4(c)(1)(iv) would require operators to identify all third-party disclosure recipients by name or category (regardless of whether disclosure is integral to the website or online service) and tell parents that they can choose not to consent to the disclosure of personal information to third parties (except to the extent such disclosure is integral to the website or online service), and because the proposed revisions to § 312.5(a)(2) would

[320] Children's Advocates Coalition, at 40.
[321] *Id.* at 24.
[322] *Id.* at 16 (explaining that "parents should also receive additional notice regarding the potential risks before giving consent for the public disclosure of their child's personal information in services like public chats, public virtual worlds, or public gaming forums.").
[323] SIIA, at 19.
[324] As defined in § 312.2 of the Rule, "third party" does not include a "person who provides support for the internal operations of the Web site or online service and who does not use or disclose information protected under this part for any other purpose."

require operators to obtain separate consent for such disclosures, operators must distinguish between disclosures to third parties that are integral to the website or online service and those that are not.[325]

iii) The Commission Adopts New § 312.4(c)(1)(iv)

After careful consideration of the record and comments, and for the reasons discussed in Part II.C.1.c.ii of this document, the Commission has decided to amend § 312.4(c)(1) to add a new paragraph (iv) as originally proposed in the 2024 NPRM, with a minor modification. For consistency with the changes described in Part II.D.1.c, the Commission is dropping the words "the nature of" from the last clause of the proposed amendments to § 312.4(c)(1)(iv) for consistency with longstanding guidance[326] and to enhance readability.

2. Section 312.4(d): Notice on the Website or Online Service

a. Proposal Related to § 312.4(d)(2)

i) The Commission's Proposal Regarding § 312.4(d)(2)

Under the current Rule, § 312.4(d)(2) requires operators to include in their online notice a description of the operator's disclosure practices for children's personal information. In the 2024 NPRM, the Commission proposed amending § 312.4(d)(2) to expressly require that operators include in their online notice "the identities or specific categories of any third parties to which

[325] The Commission notes that this paragraph uses the phrase "integral to the website or online service" rather than the language proposed in the 2024 NPRM, which utilized the phrase "integral to *the nature of* the website or online service" (emphasis added). As discussed further in Part II.C.1.c.iii, the Commission is adopting an amendment to § 312.4(c)(1)(iv) to include the phrase "integral to the website or online service," and therefore uses that phrase here.
[326] *See* COPPA FAQs, FAQ Section A.1 (noting that operators covered by the Rule must give parents the choice of consenting to the operator's collection and internal use of a child's information but prohibiting the operator from disclosing that information to third parties (unless disclosure is integral to the site or service, in which case, this must be made clear to parents)).

the operator discloses personal information and the purposes for such disclosures," and "the operator's data retention policy as required under § 312.10."[327]

ii) Public Comments Received in Response to the Commission's Proposal Regarding § 312.4(d)(2)

Many commenters generally supported the Commission's proposed amendments to § 312.4(d)(2) and the additional transparency about operators' personal information disclosure and retention practices that the proposed amendments would require.[328]

As discussed in Part II.C.1.c.ii, a wide range of commenters opined that the third parties to which the operator discloses personal information and the purposes for such disclosures are important considerations for parents.[329] Many commenters supported the Commission's proposed requirement that operators include the identities or specific categories of any third-party disclosure recipients in the online notice describing the operator's information practices.[330] A few commenters welcomed the proposal's use of the "or" conjunction (i.e., "the identities or specific categories"),[331] opining that the names of particular third parties "are unlikely to be important to parents" in some circumstances,[332] and that requiring operators to identify third-

[327] 89 FR 2034 at 2073-2074. *See also id.* at 2050 (stating "the Commission believes that this information will enhance parents' ability to make an informed decision about whether to consent to the collection of their child's personal information").
[328] *See, e.g.*, Children's Advocates Coalition, at 37-38; Consumer Reports, at 9; EPIC, at 8.
[329] *See* Part II.C.1.c.ii.
[330] *See, e.g.*, M. Bleyleben, at 5; Children and Screens, at 4.
[331] *See, e.g.*, CCIA, at 7 ("To ensure that the Rule's existing notice requirements remain clear and consistent, CCIA recommends that operators should be able to identify the categories of those third parties and rely upon their existing privacy and security programs for purpose limitation.").
[332] Engine, at 2 ("Internet companies, especially startups, rely on many types of third parties to build and make their services available to end users—for example, to provide cloud hosting, storage, or other infrastructure. Many of the third parties in a [startup's] technology stack are unlikely to be familiar to parents, like content delivery networks or software development kits, etc. In the interest of maintaining clear and concise direct notices that both ease burdens on startups and place parents' attention on truly important disclosures, this information should be relayed in the online notice. Moreover, the particular third-party services, so long as they maintain the confidentiality, security, and integrity assurances required by other areas of the COPPA rule, are unlikely to be important to parents, and therefore make most sense disclosed as categories.").

party disclosure recipients by name "could prove to be challenging for some businesses, as the identities of third parties may be subject to frequent change."[333] Other commenters, however, urged the Commission to require that operators identify the third-party disclosure recipients in the operator's online notice by name and category, explaining that identification by name and category was "essential to informed consent" and in line with legislation in other jurisdictions.[334]

Considering the potentially significant privacy implications of an operator's disclosure practices,[335] the Commission believes that parents who navigate to an operator's online notice to learn more about how the operator will handle their child's personal information should be provided with the names and categories of any third-party disclosure recipients. Besides improving parents' ability to make informed decisions about the websites or online services their children use, the Commission believes that requiring operators to describe any third-party disclosure recipients by name and category in the operator's online notice will also facilitate enhanced accountability for operators.[336] Accordingly, the Commission has decided to revise

[333] CIPL, at 11 ("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.") (emphasis in original).
[334] Common Sense Media, at 8-9 ("[R]ather than merely listing the names of third parties that operators share data with, or listing categories alone, Common Sense supports a further amendment to the rule which would require operators to organize the third parties they share data with into categories based on their function or service and identify them."). *See also* Children's Advocates Coalition, at 41-42 ("We advise the Commission to maintain its original proposal and require individual identification of third parties by name, organized by category, as defined by the FTC. This requirement provides the necessary specificity that allows parents and advocates to evaluate an operator's practices for personal comfort and legal compliance."); Consumer Reports, at 9 ("The third parties with which a operator shares personal data is likely one of the key decision points upon which parents evaluate their consent choices (for example, whether the operator shares personal data with social media companies or data brokers). . . . In recent years, Consumer Reports has advocated for privacy laws to require the disclosure of specific third parties with which covered entities share personal data on consumer transparency grounds, as well as the fact that such disclosures make assessing compliance easier for both regulators and consumer advocates.").
[335] *See, e.g.*, Part II.C.1.c.ii.
[336] *See, e.g.*, J. Chanenson et al., at 1-2 ("This approach aligns with the contemporary trend of digital transparency, empowering children and their parents to make informed decisions about their privacy. Furthermore, required third-party disclosure in the online notice enhances the longevity and accessibility of the information, ensuring that researchers can reference and track changes over time, contributing to a more robust and insightful analysis of privacy practices in the digital landscape.").

proposed § 312.4(d)(2) to require that operators' online notices identify any third-party disclosure recipients by name and category.

Several commenters also addressed the Commission's proposal to require operators to include in their online notice their data retention policy for children's personal information. Some commenters focused on the content that operators should be required to include within these retention policies. To satisfy the requirement to provide a written children's data retention policy in the § 312.4(d) online notice,[337] the Center for Democracy and Technology recommended that the Commission specify that the operator must connect the use and purpose for each type of children's data with each type of children's data.[338] Similarly, a children's advocates coalition requested that operators be required to "[tie] each personal data element to its stated purpose," and state that the operator "will not retain personal information longer than is reasonably necessary for the specified purpose for which the data was collected, and also not for any other purpose."[339]

The current Rule requires operators to describe in their online notice how the operator uses the children's data that the operator collects.[340] The Commission agrees with the commenters that, in some instances, operators' descriptions could be most helpful to parents if each type of personal information collected is tied to a particular use or to particular uses. In other circumstances, however, that level of detail could be superfluous, so the Commission

[337] As discussed in Part II.G.c, amended § 312.10 of the COPPA Rule will require that an operator include in the operator's online notice its "written data retention policy addressing personal information collected from children" rather than a "written children's data retention policy."
[338] CDT, at 3 ("This additional specificity would avoid a situation where a company lists various types of data collected from children, then separately lists a variety of uses, with no indication of the purposes for which the specific data types are used.").
[339] Children's Advocates Coalition, at 37-38.
[340] *See* 16 CFR 312.4(d)(2) ("To be complete, the online notice of the Web site or online service's information practices must state the following: . . . (2) A description of what information the operator collects from children [. . .]; how the operator uses such information; . . . .").

declines to require that operators provide in their online notice an item-by-item matrix correlating each item of personal information collected with the particular use or uses of that item of information.

Other commenters focused on the format and placement of the operator's retention policy within the operator's online notice. Concerned about possible "clutter," kidSAFE suggested that the Commission consider allowing operators to include within their online notice a link to their data retention policy rather than the actual retention policy.[341] Another commenter, the Interactive Advertising Bureau ("IAB"), argued that the Commission 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."[342]

The Commission believes that an operator's retention policy for children's personal information must be included as part of the operator's online notice, enabling parents and other interested persons to consistently and efficiently locate the policy. To mitigate concerns that such a requirement might lead to unduly long, complex, or cluttered online notices, the Commission notes that operators may use various design features, such as expandable sections (enabling a reader to obtain more detail within a given section), or intra-notice hyperlinks (enabling a reader to quickly navigate between sections within the online notice).

iii) The Commission Amends § 312.4(d)(2)

After careful consideration of the record and comments, the Commission has decided to adopt the amendments to § 312.4(d)(2) as proposed in the 2024 NPRM, with one adjustment:

[341] kidSAFE, at 15.

[342] IAB, at 21-22 ("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.").

rather than permitting operators to include in their online notice "the identities or specific categories of any third parties to which the operator discloses personal information," operators must include the identities and specific categories of any such third parties. As discussed in Part II.C.2.a.ii, the Commission believes that requiring operators to provide the names and categories of third-party disclosure recipients will improve parents' ability to make informed decisions about the websites or online services their children use and facilitate enhanced accountability for operators.

b. New § 312.4(d)(3): Notice Regarding the Collection of Persistent Identifiers

i) The Commission's Proposal Regarding New § 312.4(d)(3)

In the 2024 NPRM, the Commission proposed adding new § 312.4(d)(3), which would require an operator's online notice to include, "[i]f applicable, the specific internal operations for which the operator has collected a persistent identifier pursuant to" § 312.5(c)(7)'s support for the internal operations exception to the Rule's verifiable parental consent requirement, "and the means the operator uses to ensure that such identifier is not used or disclosed to contact a specific individual, including . . . 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)."[343]

ii) Public Comments Received in Response to the Commission's Proposal Regarding New § 312.4(d)(3)

Some consumer advocate and industry commenters supported proposed § 312.4(d)(3) while also recommending changes to it. A children's advocates coalition expressed strong

[343] 89 FR 2034 at 2050, 2074.

support for proposed § 312.4(d)(3) and also recommended that the Commission revise the proposed section to require operators' online notices to "specify each particular internal operation(s) purpose or activity for each identifier" the operator collects pursuant to § 312.5(c)(7).[344] Similarly, another commenter recommended that an operator should be required to state the purpose for which the data will be used, rather than the purpose of the disclosure.[345] Google expressed support for the proposal, but recommended "allowing businesses to refer to categories to explain how they use persistent identifiers pursuant to the exception" and "[clarifying] that operators can provide general information about the means used to comply with the definition's use restriction."[346] Citing interest in making operators' disclosures related to their collection of persistent identifiers "easily understood and parsable, as well as scalable," Google recommended that § 312.4(d)(3) permit operators to use "categories" such as "troubleshooting and debugging" to identify the specific internal operations for which they have collected persistent identifiers under the support for the internal operations exception.[347] Google cited the same interests in recommending that the Commission clarify that operators "can provide general information about the means used to comply with" the use restrictions set forth in the COPPA Rule's definition of "support for the internal operations of the website or online service."[348]

[344] Children's Advocates Coalition, at 38. As discussed in Part II.D.6.b, other commenters raised concerns about requiring operators to provide too much detail in describing the operator's support for the internal operations practices. *See, e.g.*, NCTA, at 17 ("The specific purposes for which NCTA members may rely on COPPA's support for internal operations exception may vary on a user-by-user basis or over time. Operators may simultaneously use persistent identifiers for multiple permissible internal operations purposes, for example, for authentication, content delivery, anti-fraud measures, payment, and ad attribution.").
[345] CIPL, at 11-12.
[346] Google, at 8-9.
[347] *Id.*
[348] *Id.*

Many commenters opposed the proposed addition of § 312.4(d)(3). Several raised concerns about the technical nature of the types of activities that are considered to be "support for the internal operations," and indicated that disclosures about such activities would be "highly technical and unlikely to be useful to parents."[349] Some commenters suggested that requiring the notice to disclose the practices for which a persistent identifier is collected "could reveal confidential information, security measures, proprietary information, and trade secrets . . . [as well as] previously nonpublic security practices, which bad actors could exploit."[350] By way of example, one commenter warned that "[a]n 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."[351] Another commenter similarly opposed the disclosure requirement, suggesting that the proposed addition would do little to increase transparency for parents while undermining operators' ability to keep their platforms safe.[352] Another commenter expressed concern that the proposed amendment will potentially "create painstakingly long notices"

[349] NCTA, at 17-18; *see also, e.g.*, ESA, at 13, 20-22; Epic Games, at 12; IAB, at 17-18; CIPL, at 6-7, 10-11; NAI, at 3; SuperAwesome, at 5; SIIA, at 17; The Toy Association, at 7; ANA, at 12; ACT | The App Association, at 8.
[350] CIPL, at 6-7, 11; *see also* Epic Games, at 12 ("Operators should not be required to state the internal, and often proprietary, business decisions they make to ensure compliance."); IAB, at 17-18 ("[SFIO exception will be undermined] by requiring operators to reveal previously nonpublic security practices or fraud and theft prevention measures."); ITIC, at 6-7 ("Some of the most important activities covered by the support for the internal operations exception are operators' efforts to protect 'the security and integrity of the user, website, or online service.'"); Internet Infrastructure Coalition, at 3-4 ("Requiring such detailed disclosure of confidential business operations makes operators vulnerable … Such forced openings for bad actors at this level can have dramatically negative network security effects throughout the Internet infrastructure ecosystem."); SIIA, at 17 (warning that the proposal is overbroad and risks "compromising competitive or otherwise sensitive business information"); CCIA, at 7-8 (warning that "[m]alicious actors may be able to leverage the new information found in these notices to discover vulnerabilities" and recommending that "the Commission confirm that online notice requirements do not require operators to disclose potentially sensitive business information that could compromise the safety, security, or competitiveness of the operator and their service or website"); Chamber, at 6; NCTA, at 17-18 ("While NCTA supports the principle of transparency, requiring operators to inventory and disclose their use of persistent identifiers on a specific and real-time basis would only increase the burden and liability of operators and introduce considerable new friction into the user experience without advancing the goals of ensuring that persistent identifiers are not misused.").
[351] CIPL, at 11.
[352] ESA, at 13, 20-22.

because the proposal can be read to require the operator to disclose every internal use, and stated that the disclosure requirement would call into question whether new internal uses are considered material changes that require new consent.[353] This commenter emphasized that the proposal will be particularly burdensome for operators because it will require operators that currently do not have COPPA obligations to provide notice about internal uses that the FTC deemed, by definition, to be benign enough not to require consent.[354]

One commenter queried whether the disclosure of personal information collection and use practices would duplicate disclosures in existing privacy policies required by other laws.[355] Another commenter expressed general skepticism of the benefits of detailed disclosure requirements and stated that "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 . . . and potentially raise constitutional concerns by impairing [] access to lawful content."[356] Other commenters raised concerns about operators having to "prove a negative"[357] with respect to the proposed requirement that operators disclose "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

[353] ANA, at 12-13 (citing to the NPRM's statement that some internal uses are permitted even though the Rule does not explicitly include them).
[354] ANA, at 13.
[355] SuperAwesome, at 5. This commenter also opined that the potential benefit of requiring the direct notice to disclose information about the use of persistent identifiers for support for the internal operations "is likely to be outweighed by potential consumer confusion" because "a parent may not understand why consent is not always needed for the collection and use of a persistent identifier." *Id*. To clarify, under proposed § 312.4(d)(3), an operator would be required to include this disclosure in an online notice, not in a direct notice.
[356] IAB, at 17. It is unclear how this provision, which would require companies to include a notice in an online privacy policy indicating that they use persistent identifiers for support for internal operations purposes, would affect children's access to lawful content. Regarding the level of detail that operators must disclose to satisfy the disclosure requirement, that issue is addressed in Part II.D.6.b.
[357] NCTA, at 17; T. McGhee at 3-4.

processes that encourage or prompt use of a website or online service, or for any other purpose."[358]

iii) The Commission Adopts New § 312.4(d)(3)

After carefully considering the record and comments, the Commission adopts the proposed new § 312.4(d)(3) with modifications. For the reasons explained in Parts II.B.4.c and II.D.5.c, the Commission has decided not to adopt the proposed amendments to the definition of "support for the internal operations of the website or online service" and § 312.5(c)(4) that would specifically restrict processes or uses that "encourage or prompt use of a website or online service." Therefore, the Commission will not specifically require the online notice to include disclosure of the means operators use to ensure that persistent identifiers are not used "in connection with processes that encourage or prompt use of a website or online service" as proposed in the 2024 NPRM.

In response to questions raised about the detail the online notice must provide regarding the operator's use of persistent identifiers for support for internal operations purposes, the Commission clarifies that § 312.4(d)(3) will require an operator to disclose—in general, categorical terms—how the operator uses persistent identifiers for support for internal operations purposes.[359] Disclosure of details that would threaten security protocols or reveal proprietary information, anti-fraud practices, or trade secrets is not required.

Moreover, the Commission agrees that operators need not prove a negative. Operators must, however, explain in their online notice what policies or practices are in place to avoid

[358] 89 FR 2034 at 2074.

[359] The Commission envisions that some operators might state generally that persistent identifiers are used, for example, for ad attribution, website maintenance, data security, or user authentication, while others might choose to provide additional information.

using persistent identifiers for unauthorized purposes, such as by providing a general statement about training, data segregation, and data access and storage.

The Commission has determined that new § 312.4(d)(3), as modified and clarified, will enhance oversight of operators' use of the exception relating to support for the internal operations in § 312.5(c)(7) and therefore adopts new § 312.4(d)(3).

c. New § 312.4(d)(4): Notice Regarding Collection of Audio Files

i) The Commission's Proposal Regarding New § 312.4(d)(4)

In the 2024 NPRM, the Commission proposed a new § 312.4(d)(4) to require that when an "operator collects audio files containing a child's voice pursuant to" the audio file exception to the verifiable parental consent requirement that the Commission proposed to codify in § 312.5(c)(9), the operator's online notice must include "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[.]"[360]

ii) Public Comments Received in Response to the Commission's Proposal Regarding New § 312.4(d)(4)

One commenter sought clarification as to whether proposed § 312.4(d)(4) seeks disclosure of the purpose for which, rather than technical explanations of how, the operator uses the covered audio files.[361] In response to that comment, the Commission clarifies that proposed § 312.4(d)(4) would require an operator's online notice to describe the purposes for which the operator will use the audio files the operator collects in accord with § 312.5(c)(9) of the Rule rather than providing "technical explanations" of how the operator will use the files.

[360] 89 FR 2034 at 2074.
[361] CIPL, at 11.

A children's advocates coalition strongly supported proposed § 312.4(d)(4) and also recommended that the Commission amend the proposed language to clarify that an operator's online notice must describe the purpose for which the operator will use each covered audio file or each category of covered audio files.[362] In response, the Commission clarifies that proposed § 312.4(d)(4) would require an operator's online notice to describe the purpose for which the operator will use any audio files the operator collects in accord with § 312.5(c)(9).

iii) The Commission Adopts New § 312.4(d)(4)

After carefully considering the record and comments, and for the reasons discussed in Part II.C.2.c.ii of this document, the Commission adopts § 312.4(d)(4) as proposed.[363]

D. Section 312.5: Parental Consent

1. Proposal Related to § 312.5(a)(2)

a. The Commission's Proposal Regarding § 312.5(a)(2)

Section 312.5(a)(2) currently states that "[a]n operator must give the parent the option to consent to the collection and use of the child's information without consenting to disclosure of his or her personal information to third parties."[364] In the 2024 NPRM, the Commission proposed bolstering this requirement by adding that operators must 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. The Commission also proposed adding

[362] Children's Advocates Coalition, at 39.
[363] The Commission received a comment that recommended that the Commission expand the audio file exception to the COPPA Rule's verifiable parental consent requirement to include "other forms of media or biometrics, such as facial images" and accordingly expand proposed § 312.4(d)(4) to require that operators' online notices address their collection of those other forms of media under such an expanded exception to the verifiable parental consent requirement. kidSAFE, at 8-9. As discussed in further detail in Part II.B.3.c.i, the Commission is not persuaded that the benefits of allowing an exception for prompt deletion of children's sensitive biometric information outweighs the risk to consumers. Therefore, the Commission is not expanding the audio file exception or § 312.4(d)(4) as the commenter proposed.
[364] 16 CFR 312.5(a)(2).

language that would prohibit operators required to obtain separate verifiable parental consent for disclosures from conditioning access to the website or online service on such consent.

b. Public Comments Received in Response to the Commission's Proposal Regarding § 312.5(a)(2)

A wide range of commenters expressed general support for the Commission's proposed amendments to § 312.5(a)(2).[365] Many of these commenters emphasized that requiring separate consent for disclosure, and prohibiting operators from conditioning access on such consent, could enhance transparency and enable parents to make more deliberate and meaningful choices.[366] Several commenters noted that the Commission's proposed amendments to

[365] *See, e.g.*, Common Sense Media, at 7; J. Chanenson et al., at 2; Mental Health America, at 2; ACLU, at 19; NYC Technology and Innovation Office, at 4; Consumer Reports, at 9; Heritage Foundation, at 1; Epic Games, at 6; AFT, at 2; Kidentify, at 3; State Attorneys General Coalition, at 11. Question Fourteen in the "Questions for the Proposed Revisions to the Rule" section of the 2024 NPRM requested that commenters address whether the Commission should require operators to obtain separate verifiable parental consent prior to disclosing a child's personal information, unless such disclosure is integral to the nature of the website or online service; whether the proposed consent mechanism for disclosure should be offered at a different time and/or place than the mechanism for the underlying collection and use; whether the proposed exception from the proposed separate consent requirement for disclosures that are integral to the nature of the website or online service is clear; and whether the Rule should require operators to state which disclosures are integral to the nature of the website or online service. *See* 89 FR 2034 at 2070 (Question 14).

[366] *See, e.g.*, Mental Health America, at 2 ("The requirement that the second notice be detailed will increase transparency, providing insights as to which third parties receive young people's data and what the alleged purpose for that data sharing is. That information will shed light on opaque business practices and allow young people and their families to better understand and make informed decisions as to how their information may be used."); Sutter Health, at 3 ("By requiring separate opt-in consent for targeted advertising and prohibiting the conditioning of a child's participation on the collection of excessive personal data, the proposed amendments empower parents and caregivers to make informed decisions about their children's online activities."); Epic Games, at 6 ("Epic believes that parents can make better informed decisions about their child's data when the operator's practices are laid out for them in stages. It is appropriate that for disclosures of a child's information (which can be among the most sensitive of uses), parents be given the opportunity to stop and consider their options."); CDT, at 8 ("Limiting consent to only collection and use forces parents to either accept those risks of disclosure so children can access a website or service, or to deny children a service's benefits to avoid the risks that come with disclosure."); Kidentify, at 3 ("Many parents today who provide VPC do so in an 'all or nothing' capacity, where their only options are either to agree to the full tracking of their child for advertising purposes, or to prohibit their child from participating in the activity altogether. By empowering parents with the granular option to refuse third-party disclosures while prohibiting operators from conditioning a child's access to websites or online services on parental consent, the Commission reinforces its dedication to protecting children's privacy, empowering parents, and fostering a safer online ecosystem."); State Attorneys General Coalition, at 11 ("Separate parental consent requirements for both collection and disclosure of children's personal information will heighten child privacy. It will also avoid parental confusion by preventing parents from incorrectly assuming that collection, use, and disclosure are 'bundled' together. The new proposed rule works to allow parents to control who obtains their child's information and provides an avenue for parents to further protect their child's personal information.").

§ 312.5(a)(2) would reduce the flow of children's information to data brokers and make it more difficult for companies to target children with personalized advertising.[367]

In addition to expressing support for the proposed amendments to § 312.5(a)(2), numerous commenters opined on what a separate consent process for disclosures should look like, urging the Commission to avoid implementing the proposed § 312.5(a)(2) amendments in a way that could allow for consent to be obtained through manipulative design features or strategies.[368] Some commenters opined that the separate consent contemplated by the Commission's proposed amendments to § 312.5(a)(2) should be "offered at a different time and/or place than the mechanism for the underlying collection and use."[369] Others asserted that the Commission should take a more flexible approach to avoid frustrating parents,[370] facilitating

[367] *See, e.g.*, Mental Health America, at 2; I. Seemann, at 1.

[368] Children's Advocates Coalition, at 42 ("[T]he Commission should explicitly prohibit the use of design features or manipulative strategies, commonly referred to as dark patterns, to influence parental consent decision making."); Consumer Reports, at 10 ("Drawing from lessons learned from [state privacy] laws, we strongly urge the Commission to clearly prohibit businesses from attempting to 'game' consent by bundling unrelated consents, misleading consumers about the effect of a consent decision, and manipulating consumers through consent interfaces to make the business' preferred consent decision."); California Privacy Protection Agency, at 6 ("Combining consent for collection, use, and disclosure could potentially constitute a choice architecture that is a dark pattern under the CCPA. The [California Consumer Privacy Act Regulations] explain that bundling choices such that a consumer must consent to incompatible uses of their personal information to obtain services that they expect the business to provide impairs and interferes with the consumer's ability to make a choice."); Heritage Foundation, at 1 ("Parental consent requests should be clear and not read like a complicated terms of service agreement that is easily ignored and accepted without thorough review. Consent requests should not trick parents into accepting. For example, many cookie notices make it easier to 'accept all' rather than 'confirm my choices.'").

[369] J. Chanenson et al., at 3. *See also* Children's Advocates Coalition, at 42; State Attorneys General Coalition, at 11-12; PRIVO, at 5.

[370] *See, e.g.*, Microsoft, at 9-10 ("Given the importance of user control when it has been affirmatively exercised by the user, Microsoft believes that the Commission should consider ways to avoid having that control overridden or hindered through additional requirements which require a parent to reaffirm their already stated preference. For example, when creating a child account under Xbox, parents are asked whether they want to allow their child to have access to third party publishers' games. The default setting is off. If a parent has made an affirmative change to allow a child to access these games (which are frequently a core reason for purchasing a console), it would be cumbersome and frustrating to require that parent to restate that preference through the verified parental consent process."); ITIC, at 6 ("It would also be helpful to have further clarity on when a parent can control a child's data processing by way of affirmative changes to parental settings. For example, consent for third party disclosures should be deemed sufficient when a parent affirmatively chooses to share information with third parties as part of an operator's parental control tools – this preference should not need to be reaffirmed through a separate verified parental consent process.").

"consent fatigue,"[371] or otherwise imposing unnecessary friction.[372] At least one commenter simply sought more clarity regarding the proposed separate consent requirement's parameters.[373]

Some commenters opposed the proposed separate consent requirement altogether, arguing that it was redundant,[374] would lead to consent fatigue by imposing needless burdens on parents,[375] and would "hinder many valuable and reasonable practices beyond targeted

[371] *See, e.g.*, Center for AI and Digital Policy, at 10 ("To streamline administration and avoid perpetuating 'consent fatigue,' the [consent] mechanism for disclosure may be offered at the same time and place as the [consent] mechanism for the underlying collection and use. However, it should be clearly distinguished by being positioned in a distinctly separate section following the latter [consent] mechanism with separate affirmative consent."); ITIC, at 5 ("To avoid consent fatigue and duplication, operators should be allowed to gain consent for third-party disclosures as a distinct item that is part of the broader first-party VPC process for the underlying collection/use of personal information (such as by using a clear disclosure and checkbox)."); CIPL, at 12 ("[A]ttempting 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.").

[372] *See, e.g.*, Epic Games, at 6 ("Epic would suggest [] that, to reduce friction and provide as seamless an experience for parents as possible, operators be permitted to present the separate consent for third party disclosures in the same flow as the permission for the operator's own internal uses . . . Such a rule will enable operators of well-established services to make their parental consent features and related parental controls available to third parties, many of which are small companies that have limited ability to invest in building advanced regulatory compliance systems."); ACT | The App Association, at 7 ("We encourage FTC to ensure that its rules do not introduce unneeded friction into the VPC process. For example, the App Association supports the FTC's COPPA rules allowing operators to gain consent for third-party disclosures as part of the broader first-party VPC process for the underlying collection/use of personal information (e.g., a disclosure and checkbox). Further, once a parent has provided consent to a third party to make disclosures through parental controls settings, this choice need not be reaffirmed separately in the VPC process.").

[373] *See* Taxpayers Protection Alliance, at 3 ("The FTC should specify whether consent would have to be gained for each instance of disclosure, whether this consent must be obtained in an entirely separate consent request from the consent request to gather and process data, and other expected procedures.").

[374] *See, e.g.*, Future of Privacy Forum, at 4 ("Notably, in the current COPPA rule there is already a prohibition on conditioning a child's participation in an online activity on the unnecessary disclosure of personal information. . . . Since the rule already incorporates a prohibition on the exact conduct that the separate VPC requirement in Section 312.5(a)(2) of the NPRM seeks to address, it seems that it would be a redundant requirement that does not clearly add benefit to parents and children. Therefore, FPF recommends against requiring a separate VPC for disclosure of children's data to third parties because stakeholders already face significant challenges under current VPC requirements for an operator's collection and use of child data, which a secondary VPC requirement would augment."); Scalia Law School Program on Economics & Privacy and University of Florida Brechner Center, at 18-19 ("Because parents have already consented to data collection, sharing, and use, these additional real-time notice-and-consent requirements are a needless burden. The FTC's goal in requiring another round of consent is to slow or deter the shifting of data outside the setting in which it was originally collected, but there is little reason to speculate that these secondary collections and uses—which were already subject to notice and consent—will cause harm."); ANA, at 14 ("Parents [] are already assured of the ability to provide separate consents for (1) collection and use of personal information from children and (2) disclosures of personal information to third parties. Therefore, the separate consent obligation for disclosures to third parties is unnecessary and merely creates additional work for parents.").

[375] *See, e.g.*, 4A's, at 5; The Toy Association, at 7-8; Google, at 6-7.

advertising, such as independent research activity."[376] A few commenters opposed the Commission's proposed amendments to § 312.5(a)(2) but recommended that, if the Commission nonetheless decided to implement a separate consent requirement, the Commission allow for parents to provide their consent in a streamlined fashion such as by "permitting an unchecked check box, toggle, or similar option within the initial VPC notice."[377]

Like many of the commenters that addressed the proposed amendments to § 312.5(a)(2), the Commission agrees that a separate consent requirement for non-integral disclosures to third parties, such as for third-party advertising, enhances transparency and enables parents to make more deliberate and meaningful choices, and is thus adopting the approach proposed in the

[376] Privacy for America, at 8.

[377] CARU, at 4-5 (opining that "requiring a second VPC process for disclosure will create confusion for parents and may have a chilling effect on companies that offer websites and online services to children."). *See also* Future of Privacy Forum, at 7-8 (recommending the Commission "avoid prescribing specific processes and flows for when and how the VPC for disclosure should occur" as "[o]perators' services, products, and features vary widely and thereby require different data processes and data flows which would necessitate the use of varying third parties at different times"); ESA, at 15-16 ("The proposed modification should not impose requirements that are unreasonably burdensome for parents. For example, a parent should not be required to re-start the verifiable parental consent process from scratch to consent to third-party disclosures. Instead, this separate consent to disclosure could be as simple as an affirmative action the parent must take within the existing verifiable parental consent flow. Another alternative could be for parents to use previously-provided parental passwords or pins to provide this additional consent at a later time. Moreover, many platforms and games have parental controls that allow a parent to control whether their child can disclose personal information to third parties, among other privacy and safety settings . . . Because the parent is taking an affirmative action to allow a child to disclose their personal information *after* the parent has already reviewed the operator's direct notice and provided verifiable parental consent, these settings should satisfy the additional verifiable parental consent requirement.") (emphasis in original); SIIA, at 19 ("We support incorporating the consent mechanism for [third parties'] disclosures into the broader first-party VPC process for the collection and use of personal information . . . However, capturing VPC this way is only workable if the Commission allows for reasonable implementation procedures. For example, operators should be able to use a clear disclosure and check box acknowledgment to capture VPC for disclosures to third parties as part of their own VPC for first-party collection and use."); Chamber, at 8 ("It is unclear that the COPPA statute expressly authorizes a separate disclosure requirement. But even if the COPPA statute does expressly authorize a separate disclosure requirement, the Chamber recommends that to avoid notice overloading consumers, operators should be allowed to obtain the verified parental consent for disclosure in the same notice and consent flows that they utilize in their current VPC processes."); ANA, at 14 ("Alternatively, to avoid overwhelming parents with consent requests, operators should be permitted to obtain verifiable parental consent to disclose personal information to third parties within the same interface and process used to obtain consent for collection and internal use."); Google, at 7 ("We encourage the FTC to adopt a flexible approach here to ensure any definition of 'integral' is future-proof and makes sense for different websites and online services. At the same time, we suggest that the FTC enumerate common examples of disclosures that are 'integral' across different services and likely to persist over time, such as disclosures required for legal and compliance purposes (e.g., reporting CSAM to the government) or safety purposes (e.g., reporting imminent threats to authorities).").

NPRM in the final rule, with minor language modifications as discussed in Part II.D.1.c. As to how and when such separate consent must be sought, rather than prescribe rigid requirements, the Commission is persuaded that operators should be provided sufficient flexibility to enable them to integrate the separate consent requirement in a way that enhances parents' ability to make deliberate and meaningful choices. In many contexts, seeking a parent's consent for non-integral disclosures to third parties during the initial verifiable parental consent flow may be an efficient way to obtain a parent's deliberate and meaningful consent. The Commission is persuaded, however, by the commenters that suggested operators should have the flexibility to seek parental consent for such non-integral disclosures at a later time—*e.g.*, when a child seeks to interact with a feature on the site or service that implicates non-integral third-party sharing. In that instance, the Commission expects that the operator will provide notice to the parent at the time that the parent's consent is sought so that, at minimum, the parent understands the types of personal information that will be disclosed, the identities or specific categories of third parties (including the public if making it publicly available) to whom personal information will be disclosed, and the purposes for such disclosure should the parent provide consent, and that the operator will inform the parent that the parent can consent to the collection and use of the child's personal information without consenting to the disclosure of such personal information to third parties.

Regardless of whether an operator seeks a parent's consent for non-integral disclosures to third parties during the initial verifiable parental consent flow or at a later time, the key question is whether a parent's consent to the underlying third-party disclosures is freely given, informed, specific, and unambiguously expressed through an affirmative action distinct from the parent's consent to the operator's collection and use of their child's personal information. To be clear,

consent flows that mislead, manipulate, or coerce parents—including choice architectures that deceive parents about the effect of a consent, or trick parents into providing their consent—will not suffice.[378]

Moving beyond whether separate consent should be required and what form it should take, a few commenters asserted that the Commission should require operators to obtain separate parental consent before disclosing children's personal information to entities that might not meet the Rule's definition of a "third party" (and thus would fall outside the scope of the proposed separate consent requirement).[379] Other commenters urged the Commission to ensure that various sharing scenarios were treated as disclosures covered by the proposed separate consent requirement.[380] A children's advocates coalition, for example, described at length how companies use "data clean rooms," "collaborative data sharing strategies," and "various marketing 'partnerships'" to allow marketers to "match" their data with that collected by operators covered by the Rule.[381]

---

[378] *See* 16 CFR 312.4(a) (stating "[i]t shall be the obligation of the operator to provide notice and obtain verifiable parental consent prior to [. . .] disclosing personal information from children," and providing that "[s]uch notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials").

[379] *See, e.g.*, Sandy Hook Promise, at 3 ("[W]e recommend that companies be required to obtain separate parental consent for external or partnered companies that may not qualify as third-parties. Companies often partner directly or own several platforms, which may allow them to utilize predatory data practices as their data sharing relationships do not rise to the definition of 'third-party sharing.'"); EPIC, at 10 (arguing that "[f]or the proposed Rule to be the most effective in mitigating privacy and data security harms to children, the term 'third party' should be revised to encompass *any* external entity—including operators. Currently there is no mechanism to regulate sharing with an external entity that is not a third party (as that term is defined by the Rule) . . . As it stands now, any external entity that could be considered an operator would not be a third party. The consequences for excluding operators and other external entities from the definition of third party are significant."). In response to these comments, the Commission notes that, for purposes of determining whether a disclosure has been made to a "third party," where a third party is liable directly as an operator because it has actual knowledge that it is collecting information directly from users of a child-directed website or online service, that party is still a "third party" with respect to the operator with which the child is interacting—i.e., that party is still considered a "third party" even if it is also an operator under the first prong of the "third party" definition.

[380] *See, e.g.*, Children's Advocates Coalition, at 16-22.

[381] *See id.* (emphasizing that "[u]nder COPPA, data clean rooms and associated practices should only be allowed with a separate parental consent for disclosures to third parties, as required under 312.5(a)(2)").

The Commission believes proposed § 312.5(a)(2) would sufficiently cover the entities described by these commenters given how the Rule defines the terms "Operator," "Person," and "Third party." The Rule's definition of "Operator" covers the "person" who operates the subject website or online service, where "Person" is defined as "any individual, partnership, corporation, trust, estate, cooperative, association, or other entity."[382] And the Rule defines "Third party" as "any person" who is neither an operator of the subject website or online service nor "a person who provides support for the internal operations" of the subject website or online service.[383] Accordingly, where an operator of a child-directed website or online service has allowed a third party to collect personal information through the operator's child-directed website (for example, via an advertising or social networking plug-in), the third party is still a "third party" with respect to the operator of the child-directed website or online service regardless of whether the third party might be liable directly as an operator (i.e., because it has actual knowledge that it is collecting personal information directly from users of a child-directed site or service).[384] This means that operators of child-directed websites and services would have to obtain separate consent from parents before disclosing a child's personal information to any entity other than the one providing the subject website or online service (or providing support for the internal operations of the subject website or online service).

The Commission also believes proposed § 312.5(a)(2) would sufficiently cover the sharing scenarios described by commenters given how the Rule defines "Collect" and

[382] 16 CFR 312.2.
[383] *Id.*
[384] *See, e.g.*, 78 FR 3972 at 3975-77 (describing providers of plug-in services that collect personal information from users through child-directed sites and services as "independent entities or third parties" with respect to "the child-directed content provider;" modifying the definition of "operator" to hold the operator of "the primary-content site or service" strictly liable "for personal information collected by third parties through its site;" and explaining that "it cannot be the responsibility of parents to try to pierce the complex infrastructure of entities that may be collecting their children's personal information through any one site").

"Disclose." Under the Rule, "Collects or collection means the gathering of any personal information from a child by any means,"[385] and "Disclose or disclosure means, with respect to personal information: (1) the release of personal information collected by an operator from a child in identifiable form for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the Web site or online service. . . . "[386] Accordingly, an operator that releases personal information collected from a child to a third party (other than for support for the internal operations of the operator's site or service) for a non-integral purpose would have to first obtain separate consent from parents, regardless of whether the release occurs through a so-called "data clean room," "collaborative sharing strategy," or "marketing partnership."[387]

Many commenters additionally provided their views on what types of disclosures the Commission should consider "integral to the nature of the website or online service," and some commenters urged the Commission to require separate consent regardless of whether the underlying disclosures were integral.[388] Several commenters requested that the Commission provide further clarity, and some identified particular disclosures that they believe should never be considered "integral to the nature of the website or online service," such as disclosures for advertising purposes[389] or for training or developing artificial intelligence technologies.[390] One commenter requested the Commission limit the separate consent requirement "to only third-party advertisers, not third-party service providers," asserting that many operators subject to the Rule

[385] 16 CFR 312.2.
[386] *Id.*
[387] For example, an operator that allows an advertiser to match data held by the advertiser with data collected by the operator using persistent identifiers, email addresses, or other elements of personal information will have disclosed personal information to the advertiser and would thus first need to obtain separate consent from parents.
[388] *See* Children's Advocates Coalition, at 15; Parent Coalition for Student Privacy, at 13.
[389] *See, e.g.*, Common Sense Media, at 8; State Attorneys General Coalition, at 12.
[390] *See, e.g.*, Center for AI and Digital Policy, at 10; Common Sense Media, at 8.

"rely on third-party service providers to operate their businesses, and need to share the data the operator[s] collect[] with those service providers to function."[391] As an alternative, another commenter suggested the Commission should allow operators "the opportunity to define which disclosures are integral to their service" while providing "guidance on what could be claimed as an integral third-party use and disclosure" and requiring operators "to state which disclosures are integral in their direct notice to parents."[392]

Some commenters observed that the proposed separate consent requirement could create potential complications for platform providers that host services developed by third parties. One commenter, for example, asked whether parents would be required to provide separate consent for each login to a new child-directed website or online service by their child using an email service.[393] Another commenter, the Entertainment Software Association ("ESA"), asserted that the disclosure of children's personal information between game publishers and the operators of console, handheld, mobile device, and app store services "is integral to the functioning of online video game services" because, "[f]or a child user to have a properly functioning experience in a third-party game, the platform may need to disclose certain player information along with information such as parental controls and permissions to access certain purchased entitlements

[391] CARU, at 5 (opining that "[i]f the FTC decides not to narrow the scope of third parties, this will have an outsized impact on smaller businesses"); *see also* NCTA, at 19-20 ("The FTC intimates that its primary concern underpinning this proposal is the disclosure of persistent identifiers 'for targeted advertising purposes, as well as disclosure of other personal information for marketing or other purposes.' If this is the case, then COPPA could require separate consent solely for behavioral advertising.").

[392] Future of Privacy Forum, at 7.

[393] kidSAFE, at 9 (". . . kidSAFE wonders to what extent this requirement would apply to platform providers, especially those that offer opportunities to share data with third party developers on their platform. For example, suppose a child is prompted to login with their COPPA-compliant Gmail account on a third party child-directed website, and as part of that login, the child's email address and other personal information may be shared with the third party site. Would a parent be required to provide separate consent to each such login and data sharing request, if the parent has already consented to the initial collection and sharing by Google? . . . Perhaps, therefore, this would be another good example of when the disclosure is integral to the nature of the website or online service."). *See also* Microsoft, at 9-10 (noting that parents creating child Xbox accounts are asked whether the parent wants "to allow their child to have access to third party publishers' games," and opining that "it would be cumbersome and frustrating to require th[ose] parent[s] to restate that preference").

along to the game publisher."[394] Citing a similar example, Consumer Reports noted that "a video game platform that allows third-party brands to create virtual worlds should be able to disclose personal data to that brand necessary to allow that virtual world to load," but suggested the Commission "clarify that a disclosure to a third-party is 'integral' to the nature of the website or online service when it is functionally necessary to provide the product or service the consumer is asking for."[395] Consumer Reports further urged the Commission to make clear "that the sale or sharing of personal information for consideration (monetary or otherwise) shall never be considered 'integral' to the nature of the website or service."[396] Lastly, writing in support of the proposed separate consent requirement, a large video game developer asked the Commission to "refrain from engaging in an effort to itself define those disclosures [that] are integral" because any such definition "will either be too narrow to account for the varied nature and purposes of websites and online services, or else be so broad as to be no more instructive than the plain meaning of 'integral.'"[397]

The Commission agrees that disclosures to third parties that are necessary to provide the product or service the consumer is asking for are integral to the website or online service and would not fall within the scope of the proposed amendments to § 312.5(a)(2). Of course, operators would have to identify such disclosures in the notices required under §§ 312.4(c)(1)(iv) and 312.4(d). Disclosures of a child's personal information to third parties for monetary or other consideration, for advertising purposes, or to train or otherwise develop artificial intelligence

[394] ESA, at 15.
[395] Consumer Reports, at 10; *see also* State Attorneys General Coalition, at 12 ("One proposed definition could be—the minimum disclosure necessary to effectuate the transaction, as reasonably expected by the consumer/parent.") (emphasis removed).
[396] Consumer Reports, at 10.
[397] Epic Games, at 6-7 (noting "COPPA has long included the concept of integral disclosures but has left to operators the flexibility to define for themselves what activities they deem integral").

technologies, are not integral to the website or online service and would require consent pursuant to the proposed amendments to § 312.5(a)(2).

c. The Commission Amends § 312.5(a)(2)

After carefully considering the record and comments, and for the reasons discussed in Part II.D.1.b of this document, the Commission adopts the amendments to § 312.5(a)(2) as originally proposed, with two minor modifications. The Commission is persuaded by certain commenters' overall calls for clarity on this provision. Therefore, the Commission is dropping the words "the nature of" from the first sentence of the proposed amendments to § 312.5(a)(2) for consistency with longstanding guidance[398] and to enhance readability.[399] In addition, the Commission is dropping "…and the operator may not condition access to the website or online service on such consent" from the second sentence of the proposed amendments to § 312.5(a)(2) to avoid potential confusion with a long-standing Commission position. In its 1999 Notice of Proposed Rulemaking, the Commission noted that § 312.5(a)(2) "ensures that operators will not be able to condition a child's participation in any online activity on obtaining parental consent to disclosure to third parties."[400] Given this previous declaration of § 312.5(a)(2)'s requirements regarding conditioning access, the Commission is dropping the above-referenced language to clarify that operators' obligations remain the same regarding the prohibition against conditioning participation on obtaining consent to disclosures.

---

[398] *See* COPPA FAQs, FAQ Section A.1 (noting that operators covered by the Rule must give parents the choice of consenting to the operator's collection and internal use of a child's information but prohibiting the operator from disclosing that information to third parties (unless disclosure is integral to the site or service, in which case, this must be made clear to parents)).

[399] Regarding certain commenters' request for the Commission to identify particular disclosures that are "integral" to the website or online service, the Commission notes that this is a fact-specific inquiry that depends on the type of services offered by the website or online service. The Commission agrees with other commenters that noted that any attempt to identify particular disclosures may be over- or under-inclusive depending on the website or online service, and therefore the Commission declines to provide such guidance.

[400] Children's Online Privacy Protection Rule, Notice of Proposed Rulemaking, 64 FR 22750 at 22756 (Apr. 27, 1999), available at *https://www.govinfo.gov/content/pkg/FR-1999-04-27/pdf/99-10250.pdf*.

2. Proposal Related to § 312.5(b)(2)(ii)

a. The Commission's Proposal Regarding § 312.5(b)(2)(ii)

Section 312.5(b) of the COPPA Rule governs "[m]ethods for verifiable parental consent."[401] Section 312.5(b)(2)(ii) currently states, in relevant part, "Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include: . . . (ii) Requiring a parent, in connection with a monetary 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[.]" In the 2024 NPRM, the Commission proposed to delete the word "monetary" from § 312.5(b)(2)(ii).

b. Public Comments Received in Response to the Commission's Proposal Regarding § 312.5(b)(2)(ii)

The Commission received numerous comments in support of this proposed amendment.[402] The consensus was that removing the requirement that operators charge a parent a monetary fee in order to obtain verifiable parental consent under this method "will help ease parental burden and help streamline the consent process."[403]

Opposition to the proposal came from one FTC-approved COPPA Safe Harbor program, which framed the proposed amendment as "a step backwards," as it would allow "permissioning at the highest level of assurance without any transparency to the parent or accountability by the service."[404] The commenter shared that, "when the credit card method is offered, up to 11% of the time, parents will use it when they know that the charge will be refunded."[405] The Safe

[401] As an initial matter, the Commission recommends that operators offer consumers at least a couple of different methods that the parent can use to provide verifiable parental consent.
[402] *See* CIPL, at 13; Chamber, at 9; ESRB, at 21; ACT | The App Association, at 7; kidSAFE, at 9; Advanced Education Research and Development Fund, at 8; TechNet, at 4; Epic Games, at 5.
[403] Chamber, at 9; *see also* Epic Games, at 5.
[404] PRIVO, at 5.
[405] *Id*.

Harbor program also stated that the Commission should not allow the use of debit cards as a verification mechanism, as proposed in the NPRM, because debit cards (as well as gift cards) increasingly "are available to and used by children under 13."[406]

With respect to the concerns raised by the FTC-approved COPPA Safe Harbor program, while the Commission recognizes that debit cards are now more widely available to teens than in the past, the comment did not cite data indicating that debit cards are available to children under 13. With respect to the 11% figure of parents who are willing to accept a credit or debit card charge on the basis that the charge will be refunded, that option is still available to operators, but the Commission's proposed approach would allow a credit or debit card, or other qualifying online payment, to be used without requiring the operator to enter a monetary charge and subsequently refund the amount of the charge. The Commission expects that more parents would be willing to use this option to provide verifiable parental consent if the monetary charge requirement is dropped. The Commission believes the proposed amendment could help eliminate a barrier to some parents providing verifiable parental consent while still ensuring that the use of credit cards, debit cards, or other online payment systems that provide the primary account holder with notification of each discrete transaction meets § 312.5(b)'s requirement that verifiable parental consent methods "must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent."[407]

c. The Commission Amends § 312.5(b)(2)(ii)

After carefully considering the record and comments, and for the reasons discussed in Part II.D.2.b of this document, the Commission adopts the amendment to § 312.5(b)(2)(ii) as originally proposed.

---

[406] *Id*.
[407] 16 CFR 312.5(b)(1).

3. New § 312.5(b)(2)(vi): Knowledge-Based Authentication Method for Obtaining Verifiable Parental Consent

In the 2024 NPRM, the Commission proposed adding to COPPA Rule § 312.5(b)(2)'s list of approved verifiable consent methods two methods that the Commission approved pursuant to the process set forth in § 312.12(a) after the Commission last amended the COPPA Rule in 2013.[408]

a. The Commission's Proposal Regarding New § 312.5(b)(2)(vi)

The Commission proposed adding to the Rule a new § 312.5(b)(2)(vi) that would codify as an approved verifiable parental consent method the use of a knowledge-based authentication process that meets the particular criteria the Commission approved in December 2013.[409] Such a knowledge-based authentication process entails "[v]erifying a parent's identity using knowledge-based authentication, provided: (A) the verification process uses dynamic, multiple-choice questions, where there are a reasonable number of questions with an adequate number of possible answers such that the probability of correctly guessing the answers is low; and (B) the questions are of sufficient difficulty that a child age 12 or younger in the parent's household could not reasonably ascertain the answers."[410]

b. Public Comments Received in Response to the Commission's Proposal Regarding New § 312.5(b)(2)(vi)

Several commenters supported the Commission's proposal to codify such a knowledge-based authentication process as an approved verifiable parental consent method.[411]

---

[408] 89 FR 2034 at 2053.
[409] *Id.* & n.221 (citing *FTC Letter to Imperium, LLC* (Dec. 20, 2013), available at *https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-grants-approval-new-coppa-verifiable-parental-consent-method/131223imperiumcoppa-app.pdf*).
[410] 89 FR 2034 at 2074.
[411] *See, e.g.*, CIPL, at 13; ESRB, at 21; ACT | The App Association, at 7; The Toy Association, at 7.

Although it generally supported the overall proposal to codify knowledge-based authentication as an approved verifiable consent method, FTC-approved COPPA Safe Harbor program kidSAFE urged the Commission to omit the proposed requirement that the probability of correctly guessing the answers to the dynamic, multiple-choice questions be "low."[412] kidSAFE contended that the wording of the requirement "would suggest that the [knowledge-based authentication] mechanism should be designed to be unsuccessful in obtaining consent."[413] The Commission disagrees with that concern. As stated earlier, the criteria the Commission approved in 2013 require the party employing a knowledge-based authentication process to "use[] dynamic, multiple-choice questions, where there are a reasonable number of questions with an adequate number of possible answers such that the probability of correctly guessing the answers is low" and "the questions [are] of sufficient difficulty that a child age 12 or younger in the parent's household could not reasonably ascertain the answers."[414] The Commission believes those criteria make clear that the answers should be difficult for a child to guess, not that the answers would be difficult for the parent to provide.

c. The Commission Adopts New § 312.5(b)(2)(vi)

After carefully considering the record and comments, and for the reasons discussed in Part II.D.3.b of this document, the Commission adopts new § 312.5(b)(2)(vi) as originally proposed.[415]

---

[412] kidSAFE, at 10.
[413] *Id*.
[414] *See FTC Letter to Imperium, LLC* (Dec. 20, 2013), at 3, available at *https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-grants-approval-new-coppa-verifiable-parental-consent-method/131223imperiumcoppa-app.pdf*.
[415] Due to the adoption of new § 312.5(b)(2)(vi) and (vii) (discussed in Part II.D.4), the paragraph of § 312.5(b)(2) regarding the "email plus" method of verifiable parental consent will be redesignated as § 312.5(b)(2)(viii).

4. New § 312.5(b)(2)(vii): Face Match to Verified Photo Identification Method for Obtaining Verifiable Parental Consent

a. The Commission's Proposal Regarding New § 312.5(b)(2)(vii)

The Commission proposed codifying as new § 312.5(b)(2)(vii) a previously approved verifiable parental consent method involving the matching of an image of a face to verified photo identification, subject to the particular criteria that the Commission approved in November 2015.[416] The method entails "[h]aving a parent submit a government-issued photographic identification that is verified to be authentic and is compared against an image of the parent's face taken with a phone camera or webcam using facial recognition technology and confirmed by personnel trained to confirm that the photos match; provided that the parent's identification and images are deleted by the operator from its records after the match is confirmed."[417]

b. Public Comments Received in Response to the Commission's Proposal Regarding New § 312.5(b)(2)(vii)

Several commenters supported the Commission's proposal to codify the face match to photo identification verifiable parental consent method in the Rule.[418]

Commenters that opposed codifying this parental consent method in the Rule expressed concerns regarding privacy, the cost or accuracy of human review, and the amount of burden that operators or parents bear when using the method.[419] The Commission believes it has sufficiently

---

[416] 89 FR 2034 at 2053 & n.221 (citing *FTC Letter to Jest8 Limited (Trading as Riyo)* (Nov. 18, 2015), available at *https://www.ftc.gov/system/files/documents/public_statements/881633/151119riyocoppaletter.pdf)*.
[417] 89 FR 2034 at 2074.
[418] *See, e.g.*, CIPL, at 13; ESRB, at 21; ACT | The App Association, at 7; kidSAFE, at 10; The Toy Association, at 7.
[419] *See, e.g.*, SIIA, at 8 (stating that Commission should remove the human review requirement because it is burdensome and less accurate than automated comparison of photographic images); American Consumer Institute, at 2-4 (opposing codification of the method because it comes with "significant issues to user privacy and could be a massive burden for affected companies" due, in part, to the human review requirement; stating that small businesses would struggle to use the method); ITIC, at 2 (opposing codification of the method because of "disproportionate requirement on operators to collect and process personal information" and "create[ion of] an undue burden on

addressed the first two of those concerns with conditions it imposed and statements the Commission made when approving this parental consent method in November 2015.

First, the Commission conditioned its approval of the parental consent method on the requirements that operators must not use the information collected pursuant to the method for any purpose other than completing the verifiable parental consent process, and must destroy the information "promptly" after the verifiable consent process has been completed.[420] In light of privacy concerns that commenters raised in response to the Commission's proposal to codify the face match to photo identification verifiable parental consent method in the Rule, the Commission will modify proposed § 312.5(b)(2)(vii) so that the section states explicitly what the Commission said when it approved the parental consent method in November 2015: an operator who uses the method must "promptly" delete the parent's photographic identification and facial image after confirming a match between them.

Second, the Commission believes that human review by trained personnel can enhance the likelihood of an operator concluding correctly whether an individual pictured in a government-issued identification that technology has determined is authentic is the same as the individual pictured in a second image that technology has determined came from a live person rather than a photo.[421] As for the third concern, the Commission notes that codifying in the Rule a verifiable consent method that the Commission has already approved will not require any operator to use the method. Thus, operators will only bear costs associated with using the

---

parents, potentially acting as a barrier to allowing children to engage with otherwise age-appropriate content"); TechNet, at 6 (expressing concerns that use of the method requires disproportionate collection and processing of personal information to access a service, creates an undue burden on parents, and increases the risk of inaccuracy by requiring human review); Taxpayers Protection Alliance, at 1-2 (expressing concerns about privacy risks).

[420] *FTC Letter to Jest8 Limited (Trading as Riyo)* (Nov. 18, 2015), at 4, available at *https://www.ftc.gov/system/files/documents/public_statements/881633/151119riyocoppaletter.pdf* ("Riyo's application makes clear that information collected will be promptly destroyed and that the information will not be used for any other purpose. Approval of the proposed method is conditioned on adherence to these conditions.").

[421] *Id.* at 3.

particular method if they decide to use the method instead of using other verifiable parental consent methods that meet the COPPA Rule's standard of being "reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent."[422] Parents who do not wish to use the face match to photo identification method can let operators know, and the Commission anticipates that operators will take such feedback into account in determining which verifiable parental consent methods to offer.

The Center for Democracy and Technology recommended that the COPPA Rule state that the children's personal information security program that the 2024 NPRM proposed to require under § 312.8 must ensure the deletion of the information collected in conjunction with the newly approved verifiable parental consent methods in proposed § 312.5(b)(2)(vi) and (vii).[423] The Commission understands that a separate requirement that an operator ensure, as an element of its security program, that it has deleted information as required could be useful as a backstop. However, there are already a number of Rule provisions that require operators to delete personal information, and if operators are not deleting that information as required, then they will be liable for that failure under the relevant provision of the Rule.

The Center for Democracy and Technology also stated that the Commission should provide guidance to operators regarding how they should confirm the authenticity of government-issued IDs submitted pursuant to the face match to photo identification method.[424] The Commission notes that, when the Commission approved the method in 2015, the Commission stated that the approved method included "using computer vision technology, algorithms, and image forensics to analyze the fonts, holograms, microprint, and other details

[422] 16 CFR 312.5(b)(1).
[423] CDT, at 4
[424] *Id.*

coded in the" government-issued identification document to ensure its authenticity.[425] While operators that seek to use the face match to photo identification verifiable parental consent method need not use a particular proprietary system, the approved method requires operators to use technology such as computer vision technology, algorithms, and image forensics to analyze the parent's government-issued identification document in order to ensure its authenticity.[426] Another commenter recommended that the Commission consider requiring operators to conduct and disclose risk assessments for disparate treatment and bias before they use facial recognition technology in conjunction with the method.[427] The Commission declines to impose such a risk assessment requirement, as the requirement for human review can potentially mitigate risks. Although the Rule will not impose such a requirement, operators should be aware that the Commission has challenged as an unfair act or practice under Section 5 of the FTC Act the deployment of facial recognition technology that resulted in demonstrably inaccurate outcomes, where the company deploying it failed to heed red flags or to conduct appropriate risk assessments.[428]

c. The Commission Adopts New § 312.5(b)(2)(vii)

After carefully considering the record and comments, and for the reasons discussed in Part II.D.4.b of this document, the Commission adopts new § 312.5(b)(2)(vii) with the minor modification of stating that operators' deletion of parents' identification and images collected to use the face match to photo identification verifiable parental consent method must occur "promptly" after confirmation of a match between them.

---

[425] *Letter to Jest8 Limited (Trading as Riyo)* (Nov. 18, 2015), at 2, available at *https://www.ftc.gov/system/files/documents/public_statements/881633/151119riyocoppaletter.pdf*.
[426] *Id.*
[427] NYC Technology and Innovation Office, at 2.
[428] *See, e.g.*, Complaint, *FTC v. Rite Aid Corp.*, Case No. 2:23-cv-5023 (D.D.C. Dec. 19, 2023), at 11-13, 35, available at *https://www.ftc.gov/system/files/ftc_gov/pdf/2023190_riteaid_complaint_filed.pdf*.

5. Proposal Related to § 312.5(c)(4)

a. The Commission's Proposal Regarding § 312.5(c)(4)

Section 312.5(c) of the Rule enumerates a number of exceptions to obtaining verifiable parental consent, stating that "[v]erifiable parental consent is required prior to any collection, use, or disclosure of personal information from a child *except* as set forth in [paragraphs (1)-(8)]." Section 312.5(c)(4) sets forth an exception to obtaining verifiable parental consent "[w]here the purpose of collecting a child's and a parent's online contact information is to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child."[429] In the 2024 NPRM, the Commission proposed additional language to prohibit operators from utilizing this exception to "encourage or prompt use of a website or online service."[430] The Commission explained that the proposed amendment was intended to address concerns about children's overuse of online services due to engagement-enhancing techniques, including push notifications.[431]

b. Public Comments Received in Response to the Commission's Proposal Regarding § 312.5(c)(4)

Some commenters supported the proposed amendment to § 312.5(c)(4).[432] One parent commenter supporting the proposal stated that studies have shown "a positive association with time spent on social media platforms and teen depression and suicidality."[433] Supportive

[429] 16 CFR 312.5(c)(4).
[430] 89 FR 2034 at 2059.
[431] *Id.*
[432] *See* S. Winkler, at 2; Common Sense Media, at 10-11; Heritage Foundation, at 1; Data Quality Campaign, at 4.
[433] *See* S. Winkler, at 2-3 (citing C. Vidal et al., *Social media use and depression in adolescents: a scoping review* (Feb. 17, 2020), available at *https://doi.org/10.1080/09540261.2020.1720623*).

commenters also emphasized that children are uniquely susceptible to addictive features of social media platforms, Internet games, and in-game purchases.[434]

However, a majority of commenters responding to this 2024 NPRM proposal opposed it.[435] Industry commenters argued the proposed language was overbroad and vague,[436] and would restrict beneficial push notifications and personalization, as well as features that have harmful impacts on children.[437] One commenter suggested the Commission should clarify the type of activities that would be considered encouraging or prompting the use of a website or online service, and argued that "nudging" should be permitted under the Rule as long as there is a mechanism to permit the parent to opt out of such practices by turning off the nudging feature.[438] Several commenters suggested the proposed restriction is outside the scope and purposes of the COPPA statute.[439] The American Civil Liberties Union ("ACLU") specifically contended the proposal is inconsistent with the COPPA statute because the statute provides that the Commission's regulations "shall" permit operators to respond "more than once directly to a

[434] *See* Common Sense Media, at 10-11; Heritage Foundation, at 1. *See also* Data Quality Campaign, at 4 ("Prohibiting the use of data to optimize children's attention provides an essential safeguard against digital addiction and other documented challenges.").
[435] *See* ITIC, at 6; ACLU, at 21-22; Privacy for America, at 12-14; The Toy Association, at 8; ANA, at 14.
[436] *See, e.g.*, ITIC, at 6; ANA, at 14; The Toy Association, at 8.
[437] *See, e.g.*, The Toy Association, at 8; Privacy for America, at 13. *See also* ConnectSafely, at 2 (suggesting "there are occasions where contact from the company may be appropriate even for young users, such as letting them know a friend or relative wants to chat with them…or to inform children of an important safety or security update or a new feature they might enjoy using"); E. Tabatabai, at 12-13 (discussing beneficial nudging and push notifications in ed tech products).
[438] *See* E. Tabatabai, at 13 (proposing alternative language for 312.5(c)(4) stating that "an operator may not utilize this exception to contact the child to encourage or prompt use of a website or online service unless the parent is given an opportunity to turn off or opt-out of such contact").
[439] *See, e.g.*, ConnectSafely, at 2 ("While we support efforts to prevent websites from pressuring or manipulating children to spend more time online, this appears to be outside the scope of COPPA, which was designed to protect children's data privacy."); ANA, at 14 (suggesting restriction is "outside the scope of the FTC's authority under COPPA, as the law addresses privacy and does not provide a mandate for the Commission to address or police the extent of children's online engagement"); The Toy Association, at 8 (suggesting proposal is inconsistent with the COPPA statute); Google, at 9 ("None of the objectives that COPPA was designed to achieve, or harms that COPPA was intended to prevent, have anything to do with children's engagement with online content.").

specific request from a child" when parents are provided notice and an opportunity to opt out.[440] The ACLU further suggested that instead of adding the proposed restriction, the Commission should pursue enforcement actions in appropriate cases under the existing COPPA statute and Rule where push notifications are not responsive to a "specific request" from the child or where subsequent responses are outside the scope of the child's request.[441] Several industry commenters argued the proposed amendment would violate the First Amendment rights of operators and children by restricting push notifications and other communications based on whether they contain content encouraging or prompting use of a website or online service,[442] and commenters suggested, that given the breadth of the restriction, it would likely be deemed unconstitutional under either a strict scrutiny[443] or an intermediate standard of review.[444]

c. The Commission Does Not Amend § 312.5(c)(4)

The Commission remains deeply concerned about the use of push notifications and other engagement techniques that are designed to prolong children's time online in ways that may be

[440] ACLU, at 22 ("The statutory language is mandatory and does not provide for exceptions for use cases such as push notifications, so long as the operator meets the notice and opt-out requirement. Consequently, it is not clear that the Commission has authority under the statute to amend the Rule for a specific type of repeat contacts such as push notifications or prompts.").

[441] ACLU, at 22 ("[T]he statute *does* require that the notice be in response to a 'specific request' from the child; it also limits subsequent responses to the "scope of that request.' There may be many instances where push notifications do not meet those requirements, suggesting more proactive enforcement by the Commission may be more appropriate than amending the Rule.") (emphasis added).

[442] *See, e.g.*, ANA, at 14 ("This proposed modification would unconstitutionally restrict users from receiving information about products and services and impermissibly burden commercial speech…[C]ourts have long affirmed that the First Amendment's protections include both the right of the speaker to speak and the right of the listener to receive information."); Privacy for America, at 12-14 ("The proposed prohibitions are content-based as they would disfavor protected speech with particular content such as marketing speech that encourages use of an operator's property and speech that intends to 'maximize user engagement.' Restrictions on the content of protected speech are presumptively invalid [under the First Amendment]. Only restrictions that pass strict scrutiny may be upheld.").

[443] *See, e.g.*, Privacy for America, at 12-14 (arguing strict scrutiny standard of review applies to content-based restrictions of protected speech and that Commission will not be able to satisfy its burdens of demonstrating a compelling state interest for restriction and showing that the proposal is narrowly drawn to serve that interest).

[444] *See* ANA, at 14-15 ("Regulations on commercially protected speech require the state to assert a substantial interest in protecting the speech. The regulation must directly and materially advance the state's asserted interest, and it must be narrowly tailored to serve that interest.") (citing *Central Hudson Gas & Electric v. Public Service Commission*, 447 U.S. 557, 566 (1980)).

harmful to their mental and physical health. However, the Commission also finds commenters' concerns about inconsistency between the proposal and the COPPA statute[445] and some of the First Amendment concerns related to the breadth of the proposed restriction persuasive, and therefore has decided not to adopt the proposed amendment to § 312.5(c)(4) at this time. The Commission emphasizes that the current exception set forth in § 312.5(c)(4) does not permit the collection, use, or disclosure of a child's or parent's online contact information for purposes that are not related to directly responding to a child's specific request.[446]

d. NPRM Question Fifteen: Engagement Techniques

The Commission also solicited comments about whether the Rule should be amended to address other engagement techniques and if, and how, the Rule should "differentiate between techniques used solely to promote a child's engagement with the website or online service and those techniques that provide other functions, such as to personalize the child's experience on the website or online service."[447]

Several commenters responded with a variety of suggestions. One industry commenter that opposed the amendment to § 312.5(c)(4) proposed in the 2024 NPRM indicated some support for narrower restrictions in the Rule that would impose use restrictions on techniques that solely promote a child's engagement and that would not apply to techniques that serve other functions, such as to personalize the child's experience and make content more relevant.[448] An

[445] *See* ACLU, at 22.
[446] Section 312.5(c)(4) establishes an exception to obtaining verifiable parental consent "[w]here the purpose of collecting a child's and a parent's online contact information is to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child." 16 CFR 312.5(c)(4). The Commission may take appropriate enforcement action when online contact information collected from a child, without verifiable parental consent, is used for push notifications or other purposes that are not related to directly responding to a child's specific request.
[447] *See* 89 FR 2034 at 2070-2071 (Question 15).
[448] *See* ITIC, at 6. This commenter further suggested the Commission could consider specifying that engagement techniques only fall within use restrictions (1) if they have a commercial aspect (*e.g.*, push notification promoting purchases), or (2) when they facilitate or enable access to harmful content or interactions with third parties. *Id*. However, this commenter did not suggest where or how such provisions should be incorporated into the Rule.

FTC-approved COPPA Safe Harbor program suggested the Rule "should differentiate between techniques used solely to promote a child's engagement with the website or online service and those techniques that provide other functions, such as to personalize the child's experience[.]"[449] This commenter further suggested the Commission should provide greater clarity about what engagement techniques it views as problematic, and that this might include "any use of a timer, clock, countdown visual, or engagement tracker where a prize or incentive is given for remaining on a game, activity, website or online service for an extended amount of time, or frequenting that game, activity, website or online service."[450] One non-profit organization commenter generally suggested the Rule should be amended to address the use of artificial intelligence and machine learning engagement techniques, particularly artificial intelligence chatbots and deepfakes.[451] Another non-profit organization commenter proposed that the usage of recommendation systems, particularly algorithmic-driven systems, should be regulated under the Rule as problematic engagement-enhancing techniques.[452]

Another commenter suggested the Commission should develop, with appropriate experts and other stakeholders, guidelines for "minimally addictive technology practices for child-directed services."[453] This commenter further suggested that engagement techniques nudging children towards "financialized experiences," such as features inviting children to create content for financial gain or to use currency-like features, should not be permitted.[454]

---

[449] CARU, at 3. *See also* CCIA, at 10 (suggesting Rule "should differentiate between techniques used solely to promote a child's engagement with the website or online service and those techniques that provide other functions such as making the content more relevant."); Google, at 10 ("The FTC should clarify that personalization that seeks to make a service more relevant is not a technique used to encourage or prompt use of a website or online service.").
[450] CARU, at 4.
[451] Center for AI and Digital Policy, at 10. This commenter specifically suggested that a new subsection should be added to § 312.5 "that clarifies the consent requirement, and exclusion from the consent exceptions, regarding AI/ML engagement techniques." *Id.* at 11.
[452] Center for Countering Digital Hate, at 1.
[453] Internet Safety Labs, at 9.
[454] *Id.*

Given the variety, and generality, of suggestions advanced in the limited number of comments responding to Question Fifteen in the "Questions for the Proposed Revisions to the Rule" section of the 2024 NPRM, the Commission is not amending the Rule to address specific engagement techniques at this time.

6. Proposal Related to § 312.5(c)(7)

a. The Commission's Proposal Regarding § 312.5(c)(7)

Section 312.5(c)(7) sets forth the exception to the requirement to obtain verifiable parental consent when an operator is collecting "a persistent identifier and no other personal information and such identifier is used for the sole purpose of providing support for the internal operations of the Web site or online service." Under the current Rule, there is "no obligation to provide notice under § 312.4" when an operator collects and uses a persistent identifier pursuant to this exception.[455] In the 2024 NPRM, the Commission proposed to amend this exception to require that "the operator shall provide notice [in their online notices] under § 312.4(d)(3)."[456]

b. Public Comments Received in Response to the Commission's Proposal Regarding § 312.5(c)(7)

Commenters supporting the proposed amendment commended the requirement for "businesses to disclose if and when they are collecting information from a child to support internal operations, what operational purpose this serves, and affirm that it is not used for targeted advertising."[457]

[455] 16 CFR 312.5(c)(7).
[456] 89 FR 2034 at 2050.
[457] Heritage Foundation, at 2. *See also* Children's Advocates Coalition, at 38 (strongly supporting requirement that operator specify the particular internal operations for which it has collected a persistent identifier).

Commenters opposing the proposed amendment stated that publicly providing notice of data collection for the purpose of support for the internal operations would have "minimal, if any, benefit to parents," suggesting that the requirement would cause online notices to be too lengthy to be of use when they should be clear and concise;[458] could expose sensitive business information and compromise "competitiveness of the operator;"[459] could expose data security practices;[460] and would not be effective in improving COPPA compliance.[461]

The Commission is receptive to the point that lengthy notices could become less effective at empowering parents to make privacy decisions for their children. However, the Commission weighs this against its concerns that additional transparency is needed with respect to operators' use of the § 312.5(c)(7) exception and that some operators may not comply with the use restriction.[462] The Commission believes the proposed amendment will enhance accountability for operators and require them to be thoughtful about their statements relating to data collection. In response to commenters suggesting that the online notices required by the proposed amendment could expose operators' sensitive business information, or adversely impact competition or data security practices, the Commission notes that the proposed amendment to § 312.5(c)(7) does not require a detailed description of sensitive business or technical information, including how collected information is being used to support internal operations. As discussed further in Part II.C.2.b of this document, the amendments the Commission is

[458] TechNet, at 2; Privacy for America, at 8-9; SuperAwesome, at 4-5.
[459] TechNet, at 2. *See also, e.g.*, Internet Infrastructure Coalition, at 3-4 ("The Commission's desire for greater transparency can be satisfied with far less security risk and potentially anticompetitive effects by allowing operators to identify purposes in general, categorical terms and holding them accountable to those representations through their policies on data security and privacy.").
[460] TechNet, at 2; Internet Infrastructure Coalition, at 3-4.
[461] Privacy for America, at 8-9.
[462] *See also* 89 FR 2034 at 2045 ("The Commission appreciates the concerns expressed by some commenters that there is a lack of clarity in how operators implement the support for the internal operations exception and that certain operators may not comply with the use restriction.").

adopting instead require an operator that is using the § 312.5(c)(7) exception to the verifiable parental consent requirement to include in its online notice a succinct statement that the operator is collecting and using data for those categories of activity listed in § 312.2's definition of the "support for the internal operations of the website or online service," and an explanation of what policies or practices are in place to avoid using persistent identifiers for unauthorized purposes.

c. The Commission Amends § 312.5(c)(7)

After carefully considering the record and comments, and for the reasons discussed in Part II.D.6.b of this document, the Commission adopts the amendment to § 312.5(c)(7) as originally proposed.

7. New § 312.5(b)(2)(ix): Text Plus Method for Obtaining Verifiable Parental Consent

a. The Commission's Proposal Related to New § 312.5(b)(2)(ix)

In the 2024 NPRM, the Commission observed that "permitting parents to provide consent via text message would offer them significant convenience and utility," and also noted that "consumers are likely accustomed to using mobile telephone numbers for account creation or log-in purposes."[463] The Commission further explained that these considerations suggested that "operators should be able to collect parents' mobile telephone number as a method to obtain parental consent"[464] and specifically proposed an amendment to the definition of "online contact information." As previously discussed, some commenters responding to this proposal in the 2024 NPRM also urged the Commission to consider a related amendment to § 312.5(b)(2)

[463] 89 FR 2034 at 2040.
[464] *Id*.

incorporating and approving a new text message-based method for obtaining verifiable parental consent.[465]

b. Public Comments Received Related to New § 312.5(b)(2)(ix)

A number of industry commenters and one FTC-approved COPPA Safe Harbor program[466] responding to the 2024 NPRM urged the Commission to approve and add a "text plus" provision to § 312.5(b)(2) of the Rule that would allow operators to use text messages sent to a parent's mobile telephone number to obtain verifiable parental consent with requirements similar to the approved "email plus" method set forth in § 312.5(b)(2)(vi) of the current Rule.[467] Commenters supporting a "text plus" provision suggested such a method would be more convenient to parents,[468] is similar to other consent and identity verification processes commonly used by consumers and businesses,[469] and is an appropriate update in light of technological developments and the increased use of mobile telephones.[470] The Commission finds these considerations persuasive.

At least one industry commenter suggested an alternative method of verifiable parental consent, proposing that the Commission add a new provision to § 312.5(b)(2) that would merely require "[h]aving a parent reply to a message sent using the parent's online contact

---

[465] *See, e.g.*, TechNet, at 3-4; 4A's, at 4-5; Privacy for America, at 10-11; Consumer Technology Association, at 3; kidSAFE, at 2; ANA, at 15-16; Future of Privacy Forum, at 2-3; IAB, at 26. *See also* Taxpayers Protection Alliance, at 3 (requesting that FTC clarify how operators "would be expected to obtain text-message-based consent").
[466] *See, e.g.*, TechNet, at 3-4; 4A's, at 4-5; Privacy for America, at 10-11; Consumer Technology Association, at 3; kidSAFE, at 2; ANA, at 15-16; Future of Privacy Forum, at 2-3.
[467] *See* 16 CFR 312.5(b)(2)(vi).
[468] *See, e.g.*, 4A's, at 5 ("Texting is ubiquitous, convenient, and secure, making it a reasonable mechanism for consent."); Privacy for America, at 11 ("Given the ubiquitous nature of cell phone and text message communication, enabling parents to provide verifiable consent via text message is aligned with parental expectations.").
[469] *See, e.g.*, 4A's, at 5; IAB, at 25.
[470] *See* 4A's, at 5 (contending a text plus method would "effectively respond[] to evolving technology changes"); Privacy for America, at 10-11 (suggesting that "[w]hen the Commission commenced its last update to the COPPA Rule in 2011, about 83% of American adults owned a cell phone. Today, 97% of American adults own a cell phone.").

information."[471] The Commission does not believe that an operator receiving a reply in response to a single text message is a sufficiently reliable method of obtaining verifiable parental consent. As with email, a child rather than a parent may be responding to an initial text message sent by an operator to a mobile telephone number provided by a child.[472]

At least two commenters opposed the idea of amending the Rule in a way that would allow operators to use text messages to obtain verifiable parental consent.[473] These commenters expressed concerns about security risks associated with text messages[474] and difficulties that parents might have in reading and storing a consent form on a mobile telephone.[475] As discussed in Part II.B.2.b, based on the record, the Commission has concluded that security risks are comparable in text and email communications and potential difficulties in storing consent forms are present in both email communications and text messaging. Further, the Commission notes that many parents likely would use a mobile telephone to read consent forms sent via either email or text message and, in both scenarios, parents would be reviewing notice and consent documents on the same-sized screen.[476] Text messages also can be forwarded to email accounts, allowing parents who prefer to use their email accounts for storage and reference purposes an

---

[471] IAB, at 26.

[472] The Commission has previously discussed the potential problem of children short circuiting the verifiable parental consent process by either providing their own mobile telephone number to operators or obtaining access to a parent's mobile device. *See Decision on AgeCheq Inc.'s Application for Verifiable Parental Consent Method*, FTC Matter No. P155400 (Jan. 27, 2015), available at *https://www.ftc.gov/system/files/documents/public_statements/621461/150129agecheqltr.pdf*. It is for this reason that, as discussed in Part II.D.7.c, the Commission is limiting the use of the "text plus" consent method that it is approving to situations where operators will not disclose children's personal information.

[473] *See* Parent Coalition for Student Privacy, at 11; B. Hills, at 4-5.

[474] *See* Parent Coalition for Student Privacy, at 11; B. Hills, at 4.

[475] *See* Parent Coalition for Student Privacy, at 11.

[476] *See* U.S. Census Bureau, *Computer and Internet Use in the United States: 2021* (June 2024), at 3 (observing that smartphones were the most common type of computer device reported in the American Community Survey), available at *https://www2.census.gov/library/publications/2024/demo/acs-56.pdf*; Risa Gelles-Watnick, *Americans' Use of Mobile Technology and Home Broadband* (Jan. 31, 2024) (discussing survey results related to smart phone and home broadband use and noting that "[s]ome 15% of adults are 'smartphone dependent,' meaning they own a smartphone but do not subscribe to a high-speed home broadband service"), available at *https://www.pewresearch.org/internet/2024/01/31/americans-use-of-mobile-technology-and-home-broadband/*.

additional way to retain and organize text messages related to notice and providing verifiable parental consent.

c. The Commission Adopts New § 312.5(b)(2)(ix)

After carefully considering the record and comments, and for the reasons discussed in Part II.D.7.b of this document, the Commission has decided to incorporate into § 312.5(b)(2)(ix) of the Rule a new "text plus" method for obtaining verifiable parental consent that contains requirements similar to those for the "email plus" method set forth in § 312.5(2)(vi) of the current Rule. Importantly, as with the "email plus" method, the new "text plus" method can only be utilized when an operator does not "disclose" children's personal information, because both forms of communication carry a higher risk of a child impersonating a parent than do other approved methods of obtaining verifiable parental consent. Specifically, the new provision that the Commission is adding to the Rule as § 312.5(b)(2)(ix) includes the following language: "Provided that, an operator that does not 'disclose' (as defined by § 312.2) children's personal information, may use a text message coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory text message to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier text message."

8. New § 312.5(c)(9): Audio Files Exception

a. The Commission's Proposal Regarding New § 312.5(c)(9)

In the 2024 NPRM, the Commission proposed to add to § 312.5(c) a ninth category of exception to the Rule's verifiable parental consent requirement.[477] This proposed exception provides that where an operator collects an audio file containing a child's voice, and no other personal information, for use in responding to a child's specific request, and where the operator does not use such information for any other purpose, does not disclose it, and deletes it immediately after responding to the child's request, there shall be no obligation to obtain verifiable parental consent. In such case, there also shall be no obligation to provide a direct notice, but an online notice shall be required under § 312.4(d). This proposal is consistent with the Commission's 2017 enforcement policy statement regarding the collection and use of audio files containing a child's voice.[478]

b. Public Comments Received in Response to the Commission's Proposal Regarding New § 312.5(c)(9)

The Commission received some comments that supported codifying the agency's treatment of audio files in proposed § 312.5(c)(9).[479] FTC-approved COPPA Safe Harbor program kidSAFE also suggested expanding the proposed exception to include other types of biometric data. For example, kidSAFE proposed facial images or other biometrics could be temporarily used to respond to a child's request and then deleted; this could occur when a child uploads a photo of their face to generate a deidentified cartoon version of their face, or avatar, or scans their fingerprint for age verification.[480] The Commission is not persuaded that the record is

[477] 89 FR 2034 at 2058-59, 2075.
[478] *Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings*, Federal Trade Commission (Oct. 20, 2017), at 2, available at *https://www.ftc.gov/system/files/documents/public_statements/1266473/coppa_policy_statement_audiorecordings.pdf.*
[479] *See, e.g.*, Chamber, at 9; kidSAFE, at 12; The Toy Association, at 3.
[480] kidSAFE, at 12.

sufficient at this time to support broadening the scope of exceptions for which verifiable parental consent is needed beyond what was proposed in the 2024 NPRM.[481]

c. The Commission Adopts New § 312.5(c)(9)

After carefully considering the record and comments, and for the reasons discussed in Part II.D.8.b of this document, the Commission will add the audio file exception to § 312.5(c)(9) of the Rule as proposed in the 2024 NPRM.

9. NPRM Question Thirteen: Platform-Based Consent Mechanisms

The Commission noted in the 2024 NPRM that several commenters on the 2019 Rule Review Initiation recommended that the Commission encourage platforms to participate in the verifiable parental consent process.[482] In so doing, the Commission reiterated its prior statement expressing general agreement that "platforms could play an important role in the consent process."[483] Then, in Question Thirteen of the "Questions for the Proposed Revisions to the Rule" section of the 2024 NPRM, the Commission requested that commenters on the 2024 NPRM provide additional input regarding potential benefits that platform-based consent mechanisms could provide to operators and parents and steps the Commission might take to encourage the development of such mechanisms.[484]

A variety of commenters asserted that platform-based consent could benefit individual operators and parents by making the verifiable parental consent process more efficient. For example, FTC-approved COPPA Safe Harbor program kidSAFE stated that platform-based consent could help developers obtain verifiable parental consent "in a streamlined and industry-

[481] As discussed in Parts II.B.3.b and II.B.3.c.i, the Commission received a number of comments related to biometric identifiers in connection with the proposed amended definition of "personal information" and the related questions that the 2024 NPRM posed about potential exceptions related to the proposed biometric identifiers provision.
[482] *See* 89 FR 2034 at 2052.
[483] *See id.*
[484] *See id.* at 2070.

standard fashion" and "greatly alleviate the costs associated with implementing [verifiable parental consent], especially for smaller developers."[485] Common Sense Media similarly opined that "platforms, mobile device providers, or potentially even other third parties, could prove to be useful intermediaries in obtaining verifiable parental consent" by streamlining consent to help ensure that consent is fully-informed.[486] A coalition of state attorneys general further stated that a potential benefit of platform-based consent mechanisms is that they might reduce the number of times a parent would need to provide sensitive, identifying data for the purpose of providing consent.[487]

ACT | The App Association stated that some platforms already implement measures such as family plans and parental controls that "allow[] parent[s] a simplified process to see what their kids are doing on their devices and decide what limits they want to set for their children, and ensure[] that parents have meaningful notice of and control over how an app collects, uses, and discloses their children's personal information without imposing unnecessary burdens and costs on app developers."[488] Asserting that parents "welcome a clear, centralized streamlined process," Epic Games supported the "concept of platform-based notice and consent methods" and recommended that the Commission "outline the baseline features" the Commission believes such platform-based consent mechanisms must contain to meet COPPA's requirements and then solicit public comment.[489] Kidentify Pte. Ltd. stated that platforms can help standardize consent flows and urged the Commission to focus on "platform[-]agnostic" mechanisms rather than distribution platforms because of the prevalence of cross-platform online experiences.[490]

[485] kidSAFE, at 10.
[486] Common Sense Media, at 13.
[487] *See* State Attorneys General Coalition, at 10.
[488] ACT | The App Association, at 6.
[489] Epic Games, at 13.
[490] Kidentify, at 1-3.

Some commenters cited online gaming as a particular context in which platform-based consent mechanisms would be useful. The ESA stated that the process of creating an account on a game platform before accessing any game content can provide "a convenient moment for parents to receive COPPA notices and provide verifiable parental consent," whereby "[p]ublishers can provide information about their practices for the collection, use, and disclosure of children's personal information in a uniform way, such as on game pages where parents and players can access the game for the first time on the platform."[491] The ESA further opined that implementation of platform-based consent could help ease parents' confusion about why they currently must provide consent to individual publishers after they have already provided platform consent to the platform for their children to use interactive gaming features.[492]

Some commenters that supported the development of platform-based consent mechanisms raised potential implementation concerns and suggested steps that the Commission could take to address those concerns and to incentivize development of platform-based consent mechanisms. The ESA, for example, urged that the Commission should permit operators to choose between platform-level and operator-level consent rather than making platform-based consent mandatory.[493] The ESA and an individual commenter also posited that the Commission could help incentivize platforms to create platform-based consent mechanisms by taking steps to make clear that platforms would not be liable for third parties' actions with respect to consent.[494] Common Sense Media stated that the Commission could support development of platform-based consent methods by "creating a regulatory sandbox type environment" such as that created by an

[491] ESA, at 14.
[492] *Id.*
[493] *See id.*
[494] *See* ESA, at 14-15; T. McGhee, at 6.

international privacy agency.[495] Yoti stated that efficiency considerations support the Commission encouraging platform-level consent mechanisms but cautioned that it should keep in mind that the Commission's competition mission necessitates preventing large platforms from driving competitors from the market by locking out other providers' consent mechanism.[496]

Numerous commenters voiced skepticism about or opposed platform-based consent mechanisms. One such commenter stated that platform-based consent "opens too many doors to opaque privacy practices that would be against the interests of children and against the spirit of COPPA."[497] Along similar lines, another commenter stated that the COPPA Rule should not permit large platforms to obtain one single consent for related operators, at least in part, because larger companies' purchases of many smaller companies "mak[e] it almost impossible for a parent or guardian to know what data is being given to whom."[498] The Software and Information Industry Association opposed the "requirement of platform-based consent" and urged that the Commission "reiterate that the implementation duties remain on the developer, such that the developer—not the platform—is responsible for limiting app privileges to comply with the consents that parents provide."[499] The Computer and Communications Industry Association expressed concern that making platforms responsible for obtaining verifiable parental consent for other operators could shift liability and legal risks from developers to platforms while providing little or no benefit to parents.[500] Without definitively supporting or opposing platform-based consent mechanisms, Google expressed concern about the potential of shifting from individual operators to platforms such as app stores, operating system providers, and original equipment

[495] Common Sense Media, at 13.
[496] *See* Yoti, at 14-15.
[497] M. Bean, at 1.
[498] S. Winkler, at 3.
[499] SIIA, at 8, 18.
[500] *See* CCIA, at 8-9.

manufacturers liability for complying with COPPA and urged the Commission to provide platforms sufficient liability protections if the Commission seeks to encourage platform-level consent mechanisms.[501]

An individual commenter asserted that variations in what individual operators are asking parents to consent to make the idea of a common consent mechanism operationally difficult to implement and suggested that the Commission instead support the creation of a common age assurance mechanism, such as "a universal age API."[502] The commenter opined that the creation of a common age assurance mechanism "would be a very helpful first step in addressing the biggest gap in protecting children from harms, whether privacy or content or design-related."[503]

In light of the diverse comments that the Commission received regarding platform-based consent mechanisms, and the fact that the Commission did not include proposed language regarding such mechanisms in the 2024 NPRM, the Commission is not at this time adding language to the COPPA Rule specific to the issue of platform-based consent mechanisms. The Commission might seek additional public comment on the issue in the future.

E. Section 312.7: Conditioning Access

a. The Commission's Questions for Public Comment Regarding § 312.7

Section 312.7 of the Rule provides that "[a]n 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."[504] As the Commission noted in the 2024 NPRM, because § 312.7 is an outright

[501] *See* Google, at 7-8.
[502] M. Bleyleben, at 6.
[503] *Id.*
[504] 16 CFR 312.7.

prohibition, an operator may not collect from a child more information than is reasonably necessary for the child to participate in a game, offering of a prize, or another activity, "even if the operator obtains consent for the collection of information that goes beyond what is reasonably necessary."[505]

With respect to the scope of § 312.7, the Commission noted in the 2024 NPRM that it was considering adding new language in the section to provide that an "activity" means "any activity offered by a website or online service, whether that activity is a subset or component of the website or online service or is the entirety of the website or online service."[506] In so doing, the Commission requested comment on whether that language is consistent with the COPPA statute's text and purpose, and whether it is necessary to add such language to § 312.7 given the breadth of the plain meaning of the term "activity."[507]

The 2024 NPRM also sought public comments on additional specific questions related to § 312.7 of the Rule including: what efforts operators take to comply with § 312.7, whether the Commission should specify whether disclosures for particular purposes are reasonably necessary or not reasonably necessary in a particular context, and to what extent the Commission should consider the information practices disclosed to the parent in assessing whether information collection is reasonably necessary, given that operators generally must provide notice and seek verifiable parental consent before collecting personal information.[508]

b. Public Comments Received in Response to the Commission's Questions Regarding § 312.7

[505] 89 FR 2034 at 2060.
[506] *Id.*
[507] *Id.* at 2060, 2071 (Question 18).
[508] *Id.* at 2071 (Question 17).

Numerous advocacy organizations expressed support for the Commission's statement in the 2024 NPRM that § 312.7 is an outright prohibition on collecting more information than is reasonably necessary, even if the operator obtains consent to collect information beyond what is reasonably necessary.[509] A children's advocates coalition, for example, observed that the Commission's statement in the 2024 NPRM is consistent with previous Commission guidance, previous enforcement actions, and "the general principles of data minimization that effectuate COPPA's mandate."[510] By contrast, the Commission received no comments disagreeing with its statement.

The Commission received comments both supporting and opposing the possibility of adding new language to § 312.7 to define "activity." A wide range of commenters generally supported the definition of "activity" that the Commission presented for public comment in the 2024 NPRM.[511] Such commenters stated that the proposed language would, among other things, reduce ambiguity[512] and properly place the onus of protecting privacy on operators of websites and online services rather than on parents or children.[513]

On the other hand, commenters including trade associations, scholars, a coalition of state attorneys general, and an FTC-approved COPPA Safe Harbor Program opposed adding language to § 312.7 to define "activity."[514] Such commenters asserted, for example, that the proposed

[509] Children's Advocates Coalition, at 8; CDT, at 2; Consumer Reports, at 10; ACLU, at 2-3. *See also* AFT, at 2 (supporting restricting companies from collecting more personal information than is reasonably necessary for a child to use a platform).
[510] Children's Advocates Coalition, at 8.
[511] Children and Screens, at 5; NYC Technology and Innovation Office, at 4; Mental Health America, at 2-3; Common Sense Media, at 4-5; ACLU, at 3; Consumer Reports, at 12; CDT, at 2; Children's Advocates Coalition, at 8; Council of the Great City Schools, at 7; Yoti, at 17; J. Bogard, at 1.
[512] Children and Screens, at 5; NYC Technology and Innovation Office, at 4; Consumer Reports, at 12.
[513] ACLU, at 3.
[514] NCTA, at 21; Scalia Law School Program on Economics & Privacy and University of Florida Brechner Center, at 2-3, 6-8, 13-14; T. McGhee, at 8; State Attorneys General Coalition, at 18; kidSAFE, at 13; The Toy Association, at 5.

language constitutes an expansion of the meaning of "activity" beyond statutory intent;[515] would reduce revenue streams for, and lead to fewer and lower quality, online services for children;[516] and "could get confusing" if personal information was needed for one part of a website.[517] A coalition of state attorneys general expressed concern that defining "activity" in § 312.7 "may inadvertently introduce complexities and challenges, especially as technology continues to evolve."[518] The coalition asserted that leaving the text of § 312.7 as it currently exists and not defining the word "activity" would "allow for flexibility and adaptability as technology evolves" and "enable a more pragmatic and case-specific assessment of activities offered by websites or online services."[519] FTC-approved COPPA Safe Harbor Program kidSAFE stated that it sees no value in the Commission defining "activity" and shared its experience that operators assess on a "feature-by-feature basis" whether the data they are collecting is reasonably necessary.[520] The Toy Association similarly stated that there is not an apparent need for the Commission to define the meaning of "activity" within § 312.7.[521]

Some commenters, including some that expressed general support for defining "activity," recommended that the Commission revise, or provide more specific guidance regarding, the definition the Commission set forth in the 2024 NPRM. Mental Health America, for example, recommended that the Commission "make the implicit data minimization principles within Sections 312.7, 312.10, and 312.4 [of the COPPA Rule] expressly stated, by prohibiting operators from collecting, using, or retaining, a child's personal information unless reasonably

[515] NCTA, at 21; Scalia Law School Program on Economics & Privacy and University of Florida Brechner Center, at 13-14; T. McGhee, at 8 (the statutory language "seems to be focused on unrelated incentive-based information gathering").
[516] Scalia Law School Program on Economics & Privacy and University of Florida Brechner Center, at 2-3.
[517] T. McGhee, at 8.
[518] State Attorneys General Coalition, at 18.
[519] *Id.*
[520] kidSAFE, at 13.
[521] The Toy Association, at 5.

necessary, and only for the specific purpose for which it was collected."[522] The Centre for Information Policy Leadership ("CIPL") recommended that the Commission define "activity" with greater clarity to lower the risk of blocking legitimate and beneficial data practices.[523] It recommended, in particular, that the Commission 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."[524]

A group of scholars stated that the potential definition of "activity" the Commission set forth in the 2024 NPRM raises questions about whether the COPPA Rule permits an operator to use personal information for targeted advertising, even after obtaining verifiable parental consent.[525] The group further opined that any definition of "activity" that would prohibit targeted advertising in spite of consent would be inconsistent with §§ 312.2 and 312.5(a)(2) of the Rule, which the group interprets as permitting verifiable parental consent to use persistent identifiers for purposes other than support for the internal operations of a website or service, including for targeted advertising.[526] In contrast, Consumer Reports opined that, because the Commission has stated that it interprets § 312.7 to be an outright prohibition on the collection of personal information beyond what is reasonably necessary, it follows that "any child-directed website that contains common types of third-party behavioral tracking (e.g. third-party cookies,

[522] Mental Health America, at 3.
[523] CIPL, at 15.
[524] *Id.*
[525] Scalia Law School Program on Economics & Privacy and University of Florida Brechner Center, at 6-8.
[526] *Id.*

the Facebook pixel) on a game, offering of a prize, or another activity would . . . be in violation" of § 312.7 even if the website received verifiable parental consent for such tracking.[527]

After careful consideration of the record and comments, the Commission has decided not to add new language to § 312.7 to define "activity." Questions and concerns that commenters raised about defining "activity" in § 312.7 are substantial enough to warrant additional consideration before the Commission would add new language to define this term.

In considering defining the meaning of "activity" in § 312.7, the Commission was not attempting to categorically prohibit behavioral advertising to children where the parent has provided consent. Amended § 312.5(a)(2) of the Rule does not prohibit operators from collecting personal information to engage in targeted advertising. To do so, operators must obtain the parent's opt-in consent. If the parent chooses not to consent, the operator may not condition the child's access to the operator's website or service on the child disclosing personal information for behavioral advertising purposes, and such advertising must be off by default.[528]

Although the Commission has decided not to define the meaning of "activity" in § 312.7, the Commission notes that at least some of the potential benefits that commenters contended the Commission could provide by defining the meaning of "activity" are substantially achieved through other revisions that the Commission is making to the COPPA Rule. As discussed in Parts II.C.1.b and II.C.1.c, the Commission is amending § 312.4(c)(1)(iii) and (iv) to require that an operator's direct notice to a parent for the purpose of obtaining verifiable parental consent

[527] Consumer Reports, at 11. Similarly, Common Sense Media recommended that the Commission state that "[t]he use of a child's personal information for advertising" is never reasonably necessary and that "most if not all data that may be 'reasonably necessary' for an AI model should be de-identified and aggregated." Common Sense Media, at 5-6.

[528] A number of commenters sought or recommended that the Commission provide additional guidance as to whether an operator's collection of personal information from a child is reasonably necessary. Application of the "reasonably necessary" standard, however, is inherently fact-specific. Thus, the Commission is unable to provide the additional guidance some commenters requested.

must state, respectively, how the operator intends to use the personal information the operator seeks consent to collect from the child and, if applicable, the purposes for disclosing such personal information to one or more third parties, should the parent provide consent.[529] In addition, as discussed in Part II.C.2.a, the Commission is revising § 312.4(d)(2) to require that an operator's online notice must describe the operator's retention policy for children's personal information. And, as discussed *infra*, the Commission is revising § 312.10 both to state that an operator may retain children's personal information only for as long as is reasonably necessary for the specific purposes for which it was collected, and to require an operator to establish and maintain a written data retention policy specifying the operator's business need for retaining children's personal information and the operator's timeframe for deleting it. Taken together, these revisions will prevent an operator from retaining children's personal information for longer than necessary for the specific documented purposes for which the operator collects it and ensure that, before providing consent, a parent will receive notice of how the operator intends to use their child's personal information and a hyperlink to the operator's online notice that must describe the business need for retaining children's personal information and the timeframe for deleting it. These revisions will bolster parents' ability to make informed decisions while also implementing baseline data minimization requirements that reduce the burden on parents.

Relatively few commenters responded in particular to the Commission's question of whether it should specify whether disclosures for particular purposes are reasonably necessary or not reasonably necessary in a particular context.[530] While suggesting that the Commission could provide additional guidance and illustrative examples, a coalition of state attorneys general noted

[529] Section 312.4(d)(2) currently requires operators to state in their online notices how they use the information they collect from children and, as discussed in Part II.C.2.b, under the revisions the Commission is adopting, will also require operators' online notices to state the purposes for disclosures of the information to third parties.
[530] 89 FR 2034 at 2071 (Question 17.b).

that a "reasonably necessary" determination requires a detailed, fact-specific analysis.[531] Consumer Reports expressed support for "a framework that would allow for disclosures of personal information when they are 'reasonably necessary' to provide the service requested by the user."[532] Common Sense Media stated that the Commission should provide guidance that it should never be reasonably necessary to use a child's personal information for advertising and that most, if not all, children's data used for machine learning should be de-identified and aggregated.[533]

Commenters that responded to the Commission's question regarding the extent to which the Commission should consider the information practices disclosed to the parent in assessing whether information collection is reasonably necessary[534] generally stated that the Commission should avoid making an operator's disclosures to parents determinative of whether an operator's collection of personal information from a child was reasonably necessary.[535] The Parent Coalition for Student Privacy, for example, stated that while "[c]lear and thorough notifications should be required," they "do[] not justify collection of unreasonable amounts of data nor using it for unreasonable purposes."[536] A coalition of state attorneys general similarly stated that "the Commission should review the information practices disclosed to the parent" when seeking to determine whether an operator has complied with § 312.7 of the COPPA Rule, "but such disclosures should not be determinative in deciding whether the collection of information from the child was reasonably necessary."[537] Consumer Reports stated that the Commission should

[531] State Attorneys General Coalition, at 15-17.
[532] Consumer Reports, at 11. Consumer Reports also stated that an operator should be required to obtain separate verifiable parental consent before disclosing a child's personal information to facilitate the use of targeted advertising to monetize the operator's website. Consumer Reports, at 9-10.
[533] Common Sense Media, at 5-6.
[534] 89 FR 2034 at 2071 (Question 17.c).
[535] ACLU, at 5; Parent Coalition for Student Privacy, at 14; State Attorneys General Coalition, at 18.
[536] Parent Coalition for Student Privacy, at 14.
[537] State Attorneys General Coalition, at 18.

focus on "a comparison of the operator's stated collection activities against what the Commission contextually assesses to be the data reasonably necessary to provide the service."[538]

c. The Commission Declines to Amend § 312.7

After carefully considering the record and comments, the Commission is not making any amendments to § 312.7. Commenters' varied responses weigh against the Commission making amendments at this time.

F. Section 312.8: Confidentiality, security, and integrity of personal information

Section 312.8 of the COPPA Rule requires operators to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children" and to "take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining" the information's confidentiality, security, and integrity and provide assurances that they will do so.

a. The Commission's Proposal Regarding § 312.8

In the 2024 NPRM, the Commission proposed amendments to § 312.8 to provide additional clarity as to steps operators can take to comply with § 312.8's "reasonable procedures" standard.[539] In particular, the Commission proposed adding to § 312.8 two new paragraphs (proposed § 312.8(b) and (c)). Proposed § 312.8(b) specifies that operators must, at a minimum, establish, implement, and maintain a written children's personal information security program that contains safeguards that are appropriate to the sensitivity of personal information collected from children and the operator's size, complexity, and nature and scope of activities.[540]

---

[538] Consumer Reports, at 11-12.
[539] 89 FR 2034 at 2061.
[540] *Id.* at 2075. The paragraph is modeled on the Commission's original Safeguards Rule, which the Commission promulgated in 2002 under the Gramm-Leach-Bliley Act and then amended in 2021 to require financial institutions within the FTC's jurisdiction to take certain additional steps to protect customer data. *See generally* Standards for Safeguarding Customer Information, Final rule, 86 FR 70272 (Dec. 9, 2021), available at *https://www.regulations.gov/document/FTC-2021-0072-0001*.

Proposed § 312.8(b) further specifies that, to establish, implement, and maintain such a program, an operator must designate one or more employees to coordinate the program; conduct 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 them; design, implement, and maintain safeguards to control risks identified through the required risk assessments; regularly test and monitor the effectiveness of the safeguards in place to control risks identified through the required risk assessments; and evaluate and modify the program at least annually.[541] Proposed § 312.8(c) clarifies that operators that release children's personal information to other operators, service providers, or third parties must first "take reasonable steps to determine that such entities are capable of maintaining the confidentiality, security, and integrity of the information" and obtain written assurances that the recipients will do so.[542]

b. Public Comments Received in Response to the Commission's Proposal Regarding § 312.8

Many commenters supported the Commission's proposed revisions to § 312.8 of the Rule.[543] Such commenters stated, for example, that stronger data security safeguards will help prevent or mitigate harms that can occur after data breaches.[544] Commenters supported the way that the Commission proposed to maintain flexibility in § 312.8 such as by, among other things, stating explicitly in § 312.8 that an operator's children's personal information security program

[541] 89 FR 2034 at 2075.
[542] *Id.*
[543] Mental Health America, at 3; PRIVO, at 6; Children and Screens, at 7-8; CARU, at 5; National School Boards Association, at 5; Consortium for School Networking, at 3-4; Sutter Health, at 3; Lawyers' Committee, at 6-7; J. Tirado, at 2; Microsoft, at 13; Future of Privacy Forum, at 9; EPIC, at 11-16. *See also, e.g.*, NYC Technology and Innovation Office, at 4-5 (supporting requirement for operators to obtain third parties' written assurance that they will maintain reasonable safeguards because the requirement will enhance accountability).
[544] Mental Health America, at 3; Sutter Health, at 3.

and safeguards should take into account an operator's size, complexity, nature, and scope of activities.[545]

Some commenters recommended that the Commission specify additional requirements in § 312.8.[546] One such commenter recommended that the Commission consider including requirements such as third-party assessments or verification of information security practices, training of all employees on data security, or encryption of certain personal information.[547] Although the Commission agrees that specific safeguards recommended by some commenters might be appropriate in order for some operators to meet § 312.8's "reasonable procedures" standard, the Commission believes that proposed § 312.8(b) properly recognizes that variations in the sensitivity of the personal information operators collect from children and in operators' size, complexity, and nature and scope of activities are important considerations that inform the specific safeguards the Rule should require operators to implement.

Along the same lines as commenters that recommended the Commission should include additional specific safeguards in § 312.8, another commenter recommended that the Commission "compile best practices and carefully examine" state, federal, and international data security rules "to help avoid conflicting provisions and unnecessary duplication."[548] In response, the Commission notes that it has examined other data security rules and believes that its proposed

[545] *See* PRIVO, at 6; Microsoft, at 13.
[546] *See, e.g.*, EPIC, at 11-17; CARU, at 5. *See also generally* J. Tirado, at 2 (recommending the Commission "designate the NIST [Privacy Framework] as a preferred and approved industry framework, much like a Safe Harbor framework, to both clarify the 'reasonable procedures' standard and incentivize entities to use the NIST Privacy Framework"). Along similar lines, the Parent Coalition for Student Privacy recommended that the Rule require websites or online services that rely upon school authorization as the basis for collecting personal information from children to implement specific and enhanced security protections, such as encryption at rest and in motion, regular independent audits, the provision of the results of such audits to parents upon request, and notification of schools and parents of breaches. Parent Coalition for Student Privacy, at 3, 9-10. As discussed in Part I.A, the Commission is not finalizing at this time amendments to the Rule related to ed tech and the role of schools.
[547] *See* CARU, at 5.
[548] R Street Institute, at 4.

amendments to § 312.8 provide operators appropriate flexibility and generally avoid conflict with other data security rules.

The Electronic Privacy Information Center ("EPIC") recommended that the Commission require operators' information security programs to mitigate harms to individuals rather than harms to the operator.[549] The Commission believes that proposed § 312.8(b)'s requirements—including identifying internal and external risks to the confidentiality, security, and integrity of personal information collected from children; designing, implementing and maintaining safeguards to control those risks; and regularly testing and monitoring of the effectiveness of the safeguards—inherently compel operators to take steps to mitigate harms to individuals. Accordingly, the Commission does not believe that it is necessary for § 312.8 to refer explicitly to harms to individuals.

The Toy Association opined that the proposed requirement for operators to obtain written assurances that third parties will maintain reasonable safeguards would be unduly burdensome.[550] Relatedly, kidSAFE contended that § 312.8 currently contains a sufficient requirement for operators who release children's personal information to service providers and other third parties to obtain assurances that those parties will maintain the confidentiality, security, and integrity of the information.[551] As the Commission stated in the 2024 NPRM, the written assurance requirement that the Commission proposed clarifies that an operator cannot

[549] EPIC, at 11-16. *See also, e.g.*, Children's Advocates Coalition, at 66-67 (supporting EPIC's comments on proposed § 312.8).
[550] The Toy Association, at 8.
[551] kidSAFE, at 14.

rely solely upon oral assurances[552] to meet § 312.8's existing assurance requirement.[553] However, obtaining a written contract is not the only way an operator can satisfy the written assurance requirement. To the contrary, the 2024 NPRM noted that, in proposing the written assurance requirement, the Commission envisioned that operators would be able to rely on assurances for which there is tangible evidence, such as a written contract, an email message, or a service provider's written terms and conditions.[554] The Commission continues to believe that the proposed written assurance requirement will help provide additional protection for children's personal information while allowing operators sufficient flexibility to avoid imposing undue burdens on them.[555] Therefore, the Commission adopts the written assurance requirement as proposed in the 2024 NPRM.

Numerous commenters stated that, if an operator already maintains a general information security program that applies both to children's personal information and to other data and otherwise satisfies proposed § 312.8, the Commission should not require the operator to establish and maintain a separate children's personal information security program.[556] The ESA, for

[552] The 2024 NPRM explained that, when the Commission amended § 312.8 in 2013 "to require operators to 'take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintain the confidentiality, security, and integrity of such information, and who provide assurances that they will maintain the information in such a manner'. . . , the Commission did not intend to allow operators to rely on verbal assurances alone." 89 FR 2034 at 2061. As the context makes clear, the 2024 NPRM's reference to "verbal" rather than "oral" assurances was inadvertent.

[553] Since July 1, 2013, when the last revision of the COPPA Rule became effective, § 312.8 has required an operator to obtain assurances from any entity that collects or maintains personal information from children on the operator's behalf, or to whom the operator releases children's personal information, that the entity will maintain the confidentiality, security, and integrity of the personal information. *See* 78 FR 3972 at 3994-95, 4012.

[554] 89 FR 2034 at 2061.

[555] A commenter expressed concern about small operators' ability to comply with security requirements when they are not managing the hardware on which their site is hosted. T. McGhee, at 9. To the extent the commenter has in mind an operator relying upon another entity to collect children's personal information on the operator's behalf or an operator releasing children's personal information to another entity, the operator would be able to comply with § 312.8(c) by taking reasonable steps—such as conducting research—to determine that such other entity is capable of maintaining the confidentiality, security, and integrity of the personal information and obtaining written assurances that the entity will employ reasonable measures to do so.

[556] *See, e.g.*, ESRB, at 13 ("When an operator already has comprehensive written data security and data retention policies in place, we see no reason for requiring a separate policy or program as long the overarching policies

example, recommended that § 312.8 "make clear that a general data security program" can satisfy the proposed requirement to establish, implement, and maintain a written children's personal information security program "so long as it considers the sensitivity of children's personal information and implements appropriate safeguards as necessary to address any identified risks."[557]

Some commenters proposed the inclusion of particular language in § 312.8 consistent with that recommendation. The Future of Privacy Forum, for example, recommended that the Commission revise the proposed amendments to § 312.8 to require a "written security program that contains safeguards that are appropriate to the sensitivity of the personal information collected from children" instead of a "written children's personal information security program."[558] Along similar lines, Google recommended that the Commission permit operators to use risk assessments conducted independently of the requirements set forth in § 312.8 of the Rule to satisfy § 312.8's proposed risk assessment requirement.[559] Google asserted that the Commission's adoption of that recommendation would help prevent the Rule from imposing undue compliance burdens on operators, especially startups or small businesses.[560]

The Commission agrees that an operator should not be required to implement requirements specifically to protect the confidentiality, security, and integrity of personal information collected from children if the operator has established, implemented, and maintained an information security program that applies both to children's personal information and other information and otherwise meets the requirements the Commission proposed in § 312.8 of the

account for the heightened sensitivity of children's data and the operator implements corresponding measures."); Microsoft, at 13-14; Future of Privacy Forum, at 9; Chamber, at 11; ESA, at 19-20; IAB, at 23-24; NCTA, at 21-22; ITIC, at 7; CIPL, at 15-16; ANA, at 16; The Toy Association, at 8; Internet Infrastructure Coalition, at 4.

[557] ESA, at 19.

[558] Future of Privacy Forum, at 9.

[559] Google, at 12.

[560] *Id.*

2024 NPRM. Accordingly, the Commission is modifying the language it proposed in § 312.8 of the 2024 NPRM. In particular, in the first sentence of proposed § 312.8(b), proposed § 312.8(b)(1), and proposed § 312.8(b)(5), the Commission is changing "children's personal information security program" to "information security program." Further, the Commission is changing "[t]o establish, implement, and maintain a children's personal information security program" in the second sentence of proposed § 312.8(b) to "[t]o satisfy this requirement." And the Commission is adding to the end of proposed § 312.8(b)(5) the phrase "to protect personal information collected from children."

One commenter expressed concern that the Commission's proposed revision of § 312.8 does not make sufficiently clear the level of detail that a written children's personal information security program must contain.[561] The Commission disagrees with that concern. As set forth in the 2024 NPRM, the Commission's proposed revisions of § 312.8 state specific steps an operator must take to establish, implement, and maintain an information security program to protect personal information collected from children and criteria for determining which safeguards such a program will contain.[562] In addition, as discussed *supra*, the Commission is now providing additional clarity by making modifications to proposed § 312.8 to make clear that an operator need not maintain a separate children's personal information security program if it maintains an information security program that applies both to children's personal information and other information and otherwise meets § 312.8's requirements. The Commission believes that § 312.8, as finalized, provides sufficient guidance to facilitate operators' compliance.

Some commenters requested that the Commission clarify that the employee an operator designates to coordinate its information security program to protect personal information

[561] The Toy Association, at 8.
[562] 89 FR 2034 at 2060-61, 2075.

collected from children in accord with proposed § 312.8(b)(1) of the Rule may also have other job duties.[563] That request is consistent with the Commission's intent. The Commission therefore clarifies that § 312.8 will permit the employee an operator designates to coordinate its information security program to have additional job duties. Some commenters stated that the Commission should not require operators to publish their information security programs.[564] The Commission clarifies that it did not propose, and is not seeking to impose, such a requirement.

kidSAFE raised the concern that the Commission's proposed revisions to § 312.8 of the Rule are "extremely cost and resource prohibitive for small businesses" and will "push companies over the edge financially or lead them to turn a blind-eye to children users."[565] kidSAFE recommended that, if the Commission codifies the proposed revisions in the Rule, the Commission should apply them only to businesses that exceed certain thresholds in terms of revenues or number of employees.[566] kidSAFE did not provide evidence to support these assertions. As discussed earlier, the proposed revisions to § 312.8 include flexibility that will help ensure small businesses do not face undue burdens. Among other things, § 312.8, as finalized, states that an operator's size, complexity, and nature and scope of activities, and the sensitivity of the personal information the operator collects from children, are all pertinent factors for determining which safeguards are appropriate for the particular operator to establish, implement, and maintain. In addition, an operator need not maintain a separate children's personal information security program if it maintains an information security program that applies both to children's personal information and other information and otherwise meets

[563] CIPL, at 16. *See also generally* The Toy Association, at 8 ("In addition, businesses with smaller staff may be less able to designate employees to coordinate a security program, as such coordination would likely be in addition to employees' existing roles at the business.").
[564] Internet Infrastructure Coalition, at 4; ITIC, at 7.
[565] kidSAFE, at 13.
[566] *Id.* at 13-14.

§ 312.8's proposed requirements. And the employee who coordinates an operator's information security program in accord with § 312.8 may have additional job duties.

c. The Commission Amends § 312.8

Having carefully considered the record and comments, and for the reasons discussed in Part II.F.b of this document, the Commission adopts the revisions to § 312.8 as proposed in the 2024 NPRM, except for minor changes to make clear that an operator need not implement requirements specifically to protect the confidentiality, security, and integrity of personal information collected from children if the operator has established, implemented, and maintained an information security program that applies both to children's personal information and other information and otherwise meets § 312.8's requirements. In particular, as discussed in more detail *supra*, the Commission has modified the 2024 NPRM's proposed revisions of § 312.8 to omit references to a "children's personal information security program."

G. Section 312.10: Data Retention and Deletion Requirements

Current § 312.10 of the COPPA Rule states that "[a]n operator of a web site or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected."[567] In addition, current § 312.10 states that, when an operator deletes personal information collected online from a child, it must use "reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion."[568]

a. The Commission's Proposal Regarding § 312.10

Some commenters that responded to the Commission's 2019 Rule Review Initiation recommended that the Commission clarify operators' obligations under § 312.10. Commenters

[567] 16 CFR 312.10.
[568] *Id.*

expressed concern that, because § 312.10 does not set forth specific time limits on data retention, operators could read the COPPA Rule to allow indefinite retention of children's personal information.[569] In response to these comments, the Commission stated in the 2024 NPRM that, although the Commission framed § 312.10's prohibition on data retention to permit operators flexibility to retain data for specified business needs, § 312.10 prohibits operators from retaining children's personal information indefinitely.[570] This clarification is consistent with the complaints and orders in numerous recent FTC enforcement actions under COPPA.[571]

In addition to noting that § 312.10 is an outright prohibition against indefinite retention, the Commission proposed in the 2024 NPRM to amend § 312.10 to state more clearly operators' duties with regard to the retention of personal information collected from children. First, the Commission proposed clarifying that operators may retain children's personal information for only as long as is reasonably necessary for the specific purposes for which it was collected, and not for any secondary purpose.[572] Concomitant with that proposal, the Commission proposed

---

[569] *See* 89 FR 2034 at 2062.

[570] *See id.* ("Section 312.10 prohibits operators from retaining children's personal information indefinitely. The Commission framed the prohibition on data retention to permit enough flexibility to allow operators to retain data only for specified, necessary business needs.").

[571] *See, e.g.*, Complaint, *FTC and The People of the State of California v. NGL Labs, LLC*, Case No. 2:24-cv-05753 (C.D. Cal. July 9, 2024), at 22, 28-29, available at *https://www.ftc.gov/system/files/ftc_gov/pdf/NGL-Complaint.pdf* (alleging that Defendants retained all customer data provided to them indefinitely and thus violated COPPA by retaining data collected online from children under the age of 13 for longer than reasonably necessary); Complaint, *United States v. Microsoft Corp.*, Case No. 2:23-cv-00836 (W.D. Wash. June 5, 2023), at 7, 9-10, available at *https://www.ftc.gov/system/files/ftc_gov/pdf/microsoftcomplaintcivilpenalties.pdf* (alleging that Defendant violated COPPA by indefinitely retaining personal information collected online from children under the age of 13 who did not complete account creation process); Complaint, *United States v. Amazon.com, Inc.*, Case No. 2:23-00811 (W.D. Wash. May 31, 2023), at 3, 6-10, 14, available at *https://www.ftc.gov/system/files/ftc_gov/pdf/Amazon-Complaint-%28Dkt.1%29.pdf* (alleging that Defendants violated COPPA by indefinitely retaining personal information collected online from children under the age of 13); Complaint, *United States v. Edmodo, LLC*, Case No. 3:23-cv-02495 (N.D. Cal. May 22, 2023), at 14-17, available at *https://www.ftc.gov/system/files/ftc_gov/pdf/edmodocomplaintfiled.pdf* (alleging that Defendant violated COPPA by indefinitely retaining personal information collected online from children under the age of 13); Complaint, *United States v. Kurbo, Inc.*, Case No. 3:22-cv-00946 (N.D. Cal. Feb. 16, 2022), at 11, 14-15, available at *https://www.ftc.gov/system/files/ftc_gov/pdf/filed_complaint.pdf* (alleging that Defendants violated COPPA by indefinitely retaining personal information collected online from children under the age of 13).

[572] 89 FR 2034 at 2062, 2075.

stating in § 312.10 that operators must delete children's personal information when the information is no longer reasonably necessary for the purposes for which it was collected.[573] In addition, the Commission proposed requiring in § 312.10 that an operator must establish and maintain a written children's data retention policy specifying the purposes for which children's personal information is collected, the business need for retaining the information, and the timeframe for deleting it, precluding indefinite retention.[574] The Commission also proposed requiring in § 312.10 that operators provide their written children's data retention policies in the notices required by § 312.4(d) of the Rule.[575]

b. Public Comments Received in Response to the Commission's Proposal Regarding § 312.10

Numerous commenters stated general support for the Commission's proposed revisions to § 312.10.[576] The Center for Democracy and Technology, for example, stated that the proposed "additions to § 312.10 better emphasize operators' data minimization responsibilities."[577] Consumer Reports similarly stated that the proposed revisions would both "ensure that the data minimization protections contemplated in § 312.7 extend beyond the collection phase so that operators may not use [children's] personal information for unexpected secondary purposes, like profiling or third-party targeted advertising" and reduce the attack

[573] *Id.*
[574] *Id.*
[575] *Id.* at 2050, 2073-74. The Commission explained that the proposed revisions to § 312.10 reinforce § 312.7's data minimization requirements, which, as discussed in Part II.E.a, prohibit an operator from conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity. *See* 89 FR 2034 at 2062.
[576] *See, e.g.*, Children and Screens, at 7-8; Lawyers' Committee, at 6; Mental Health America, at 3-4; Sutter Health, at 3; Consumer Reports, at 11; CDT, at 4-5; Data Quality Campaign, at 3-4 (expressing support and also stating that it is important for § 312.10 to still enable and allow among other things, longitudinal research, school accountability, systemic school improvements, and other school-authorized education purposes); EPIC, at 16-17; AFT, at 2 (supporting proposal for the Rule to state explicitly that operators cannot retain children's personal information indefinitely).
[577] CDT, at 5.

surface for data breaches.[578] Mental Health America stated that the proposed revisions "will effectively prohibit platforms from using kids' data for secondary uses such as optimizing design features that have harmful mental health effects and will help ensure operators are not maintaining data profiles of child users indefinitely."[579] In addition to those commenters that stated general support for the proposed revisions of § 312.10, some commenters expressed support, in particular, for the Commission's proposal to amend § 312.10 to explicitly prohibit indefinite retention of personal information collected from children,[580] or to require operators to establish, implement, and maintain a written children's data retention policy.[581]

A few commenters raised questions about the "secondary purpose" language in the proposed amendments to § 312.10. The IAB asked the Commission to clarify whether the retention of children's personal information to improve products and services or to personalize content shown to children would be a "secondary purpose," and recommended that the Commission clarify in amended § 312.10 that "activities constituting 'support for the internal operations' are not secondary purposes."[582] The ACLU made a similar recommendation and posited that the Commission modifying proposed § 312.10 to state explicitly that operators may retain data as is reasonably necessary to provide support for the internal operations of the website or online service would help "avoid precluding uses that bolster privacy and security."[583] In response to these commenters, the Commission notes that proposed amended § 312.10 expressly

[578] Consumer Reports, at 11. *See also, e.g.*, CDT, at 5 ("We agree that these additions to §312.10 better emphasize operators' data minimization responsibilities. Data retention and deletion requirements go hand-in-hand with up-front minimization requirements like those in §312.7. Even when an operator legally collects data, there is little reason for indefinite retention of that data. Therefore, it is good policy to ensure that operators incorporate soup-to-nuts data practices that begin with collection limits and end with retention limits.").
[579] Mental Health America, at 4.
[580] *See, e.g.*, PRIVO, at 6 (stating that PRIVO has long implemented such a prohibition); AFT, at 2.
[581] *See, e.g.*, SIIA, at 12-13.
[582] IAB, at 22.
[583] ACLU, at 4.

permits operators to collect children's personal information for more than one specific purpose.[584] Under the proposed amended section, an operator that collects children's personal information to improve the website or online service, to personalize content shown to children on the website or online service, to provide support for the internal operations of the website or online service, or for any other purpose must set forth such purposes in its online notice, along with the business need for retaining the information, and a timeframe for deleting the information. The "secondary purpose" language was meant to encompass retention of children's personal information for any other purpose (*i.e.*, any purpose that the operator has not disclosed in its online notice)—not to suggest that retention limits must depend on a single primary purpose. Because the proposed "secondary purpose" language is unnecessary[585] and appears to have generated some confusion, the Commission has decided to omit the words "and not for a secondary purpose" from the final Rule. With that adjustment, the Commission believes that the proposed amendments to § 312.10 will provide more transparency about operators' practices without precluding data uses that support the internal operations of websites or online services or that bolster privacy and security.

A large number of commenters requested that the Commission clarify that the express prohibition on indefinite retention in the proposed amendments to § 312.10 will not prevent operators from retaining children's personal information indefinitely for purposes such as security, fraud and abuse prevention, financial record-keeping, ensuring service continuity, complying with other legal or regulatory requirements, or ensuring the age-appropriateness of

[584] For consistency, the Commission is changing "purpose" to "purposes" in the second sentence of proposed amended § 312.10.

[585] Regardless of whether the words "and not for a secondary purpose" are included, operators may only retain children's personal information for as long as is reasonably necessary to fulfill the specific purposes for which it was collected, and must delete the information when it is no longer reasonably necessary for the purposes for which it was collected.

the website or online service.[586] Along similar lines, CIPL and Epic Games each recommended that amended § 312.10 permit indefinite retention for specific use cases, such as an online gaming services' indefinite retention of a child's personal information to preserve scores, interactions, communications, user-generated content, purchases, and other transactions in accordance with the user's expectations.[587] kidSAFE recommended that the Commission revise § 312.10 to allow for indefinite retention in relation "to certain features in cloud-based productivity tools or in products for which parents have purchased lifetime subscriptions."[588] A few commenters also requested that the Commission clarify that the proposed revisions to § 312.10 will permit operators to retain children's personal information where the child user or the parent directs an operator to retain data.[589]

The Commission does not see a need to adjust its initial proposal based on these recommendations. The proposed amendments to § 312.10 would permit operators to retain

[586] *See, e.g.*, ITIC, at 7; Google, at 11-12 (requesting flexibility to retain children's personal information to comply with legal requirements like preservation letters or for security, fraud and abuse prevention, financial record-keeping, or to ensure continuity of services); SIIA, at 13 (recommending exceptions to the prohibition against indefinite retention for security, fraud and abuse prevention, financial record-keeping, complying with legal or regulatory requirements, ensuring service continuity, or ensuring the safety and age appropriateness of the service"); CCIA, at 11 (recommending exceptions for security, fraud and abuse prevention, financial record-keeping, complying with relevant legal or regulatory requirements, ensuring service continuity, or when the user has provided verifiable parental consent to the extended retention of data); ANA, at 16 (same); ACT | The App Association, at 8 (recommending exceptions for maintaining the security and integrity of the offering, preventing fraud and abuse, adhering to other legal requirements, and when a parent requests that data be retained); TechNet, at 2 (recommending exceptions for security, fraud and abuse prevention, financial recordkeeping, compliance with legal or regulatory requirements, service continuity, and efforts to ensure the safety and age-appropriateness of the service); Internet Infrastructure Coalition, at 4 (recommending flexibility for security, prevention of fraud and abuse, financial record-keeping, and continuity of service operations."); Taxpayers Protection Alliance, at 3-4 (recommending exceptions for necessary security, regulatory-compliance, safety, and anti-fraud purposes."). *See also generally* R Street Institute, at 4-5 (supporting "data minimization concepts, including data retention and deletion requirements," but opposing "broad data use restrictions that limit future innovation" and stating that a general prohibition against indefinite retention might need to provide exceptions for purposes like financial record-keeping, legal requirements, and fraud prevention);.CIPL, at 16-17 (stating that the Commission should clarify that data retention purposes such as security, fraud prevention, financial recordkeeping, legal and regulatory requirements, ensuring service continuity, and consent for extended retention of data are not "secondary purposes" under the proposed amendments to § 312.10).

[587] CIPL, at 16; Epic Games, at 12.

[588] kidSAFE, at 15 (asserting that "[t]imed deletion of user data in these cases would be unfair to parents and children, who reasonably expect that these services retain their data").

[589] *See, e.g.*, ITIC, at 7 (child user or parent); ESA, at 20 (parent); Internet Infrastructure Coalition, at 4 (parent).

children's personal information for as long as is reasonably necessary to fulfill the specific purposes for which the operator collects the information and discloses to parents. The Commission believes that the proposed revisions to § 312.10 would give operators sufficient flexibility to establish, and state in their written children's personal information retention policies, reasonable retention periods for children's personal information to satisfy any of the purposes commenters identified while ensuring that operators do not retain children's personal information indefinitely. For example, the proposed revisions would permit an operator to retain children's personal information for a specific amount of time after the child has last used the operator's website or online service, or a subscription has ended, if there is a business need for retaining the information and the operator's retention policy explains the operator will take such action.[590] However, the proposed revisions will preclude operators from retaining children's personal information indefinitely, including permanently.

Similar to comments that the Commission received in response to its proposal to revise § 312.8 to require operators to maintain a written children's personal information security program, numerous commenters urged the Commission to clarify that the proposed revisions to § 312.10 would not require operators to establish, implement, or maintain a separate, distinct written children's data retention policy as long as they maintain a general data retention policy that encompasses children's personal information.[591] The Commission does not intend to require

[590] Such a scenario is consistent both with comments that recommended that the Commission require operators' data retention policies to state data retention periods as precisely as possible and comments that advised against prescribing specific time frames for data retention. *See, e.g.*, L. Cline, at 3-5 (criticizing information retention policies that state that an operator will retain information "for as long as necessary to fulfill the business purpose" without including an enforceable end date); J. Schwarz, at 8-10 (recommending that the Commission require operators to state in "days, weeks, months, and years" the retention period for each category of data they collect); The Heritage Foundation, at 2 ("Prescribing a specific time frame for data retention creates a ceiling and encourages operators to use the maximum time allowed.").

[591] *See, e.g.*, ITIC, at 7; CCIA, at 11; Internet Infrastructure Coalition, at 4; ESRB, at 13; IAB, at 21-22; Chamber, at 11.

an operator to establish, implement, or maintain a separate written children's data retention policy if the operator has established, implemented, and maintained a written data retention policy that encompasses children's personal information and satisfies the requirements set forth in amended § 312.10, including the requirements that (1) the written data retention policy set forth the purposes for which children's personal information is collected,[592] the business need for retaining such information, and a timeframe for deletion of such information, and (2) the operator provide the policy in the online notice required by § 312.4(d) of the COPPA Rule. In response to the comments suggesting the proposed revisions of § 312.10 did not make the Commission's intent clear, the Commission is modifying the language proposed for § 312.10 in the 2024 NPRM. In particular, instead of adopting the phrase "children's data retention policy," the Commission is adopting the phrase "data retention policy." Additionally, as part of the 2024 NPRM, the Commission proposed that the final sentence of amended § 312.10 read, "The operator must provide its written data retention policy in the notice on the website or online service provided in accordance with § 312.4(d)." In finalizing the proposed amendments, the Commission is adding the phrase "addressing personal information collected from children" following the word "policy." These changes make clearer that the amended Rule will not require an operator to establish, implement, or maintain a separate written children's data retention policy if the operator has established, implemented, and maintained a written data retention policy that encompasses children's personal information and meets the requirements of amended § 312.10.

One commenter, the IAB, opined that the Commission underestimated the burden of the Commission's proposal to require operators to establish and maintain a written data retention

[592] In other words, the written data retention policy must set forth the purposes for which personal information is collected from children as distinguished from people aged 13 or older.

policy addressing personal information collected from children.[593] It recommended that the Commission reduce such burden 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."[594] But the IAB offered no supporting evidence for its assertion regarding burden, and the Commission declines to adopt its recommendation. The Commission believes that its proposal that operators' written data retention policies state the purposes for which children's personal information is collected, the business need for retaining such information, and the timeframe for deleting it will require no more than the approximately 10 hours per operator that the Commission estimated in the 2024 NPRM[595] because, to comply with the COPPA Rule and other laws and regulations, and for operational reasons, the Commission believes that many covered operators already have written data retention policies that include the same or largely the same elements that the Commission has proposed to require.[596] The IAB did not provide sufficient detail for the Commission to evaluate what it meant by a "general description of the purposes for which personal information is collected and a general statement of the operator's retention timeframes" That said, as already discussed, the Commission is adopting the recommendation of the IAB and other commenters that the Commission clarify that amended § 312.10 will permit maintenance of a general written data

[593] IAB, at 21-22. *See also generally* ANA, at 16 (stating that the proposed requirement to post a written children's personal information retention policy would "burden smaller operators disproportionately in comparison to their larger counterparts that can dedicate time and expenses to crafting, updating, and managing such a public policy").
[594] IAB, at 21.
[595] *See* 89 FR 2034 at 2066.
[596] The IAB asserted that proposed revised § 312.10 should not require operators' written children's personal information retention policies to state the "business need" for retaining children's personal information because such a requirement is "redundant" with the proposed requirement for the policies to state the purposes for collecting the personal information. IAB, at 21-22. The Commission disagrees that those proposed requirements are necessarily redundant. A business need for retaining personal information—*e.g.*, to comply with recordkeeping obligations after a user has ceased using the website or online service—may differ from the purpose for which the personal information was collected—*e.g.*, to authenticate a user seeking to log into the website or online service.

retention policy that encompasses children's personal information and otherwise meets the requirements of amended § 312.10.

Some commenters opposed § 312.10's proposed requirement for operators to publish their data retention policies addressing personal information collected from children on the grounds that the policies could contain information that is proprietary or could otherwise compromise the safety or security of a website or online service or that of its vendors, and that potential benefits to consumers do not outweigh those potential risks.[597] The Commission disagrees with that assertion. Simply put, the commenters did not provide persuasive evidence that including the required disclosures in the § 312.4(d) notices will compromise proprietary information or the safety or security of operators' websites or online services. Disclosure of the required information can help inform parents' and children's choices about which websites or online services children will use and also help ensure that operators are complying with their other obligations under §§ 312.10, 312.7, and 312.8 of the Rule.[598]

EPIC recommended that the Commission more clearly impose "both a necessity and a volume limitation" in § 312.10 by stating that an operator may retain personal information collected online from a child for only "as long as reasonably necessary and proportionate to provide the service requested by a child or parent."[599] The Commission declines to implement this recommendation in light of the protections already provided under § 312.7's prohibition against collecting from a child personal information beyond that which is reasonably necessary

[597] *See, e.g.*, ESA, at 20; Internet Infrastructure Coalition, at 4; NCTA, at 18.
[598] The Commission disagrees with NCTA's assertion that the proposed requirement for operators to post their data retention policies is "unnecessarily duplicative of existing Rule requirements [in § 312.6] that operators provide parents, upon request, with a description of the specific types or categories of personal information the operator collects from children and a means of reviewing any personal information collected from that particular child." NCTA, at 18. For example, operators' posting of their policies for retaining children's personal information will enable parents to evaluate operators' retention practices before deciding whether to consent to operators' collection of the children's personal information in the first instance.
[599] EPIC, at 16-17.

for the child to participate in an activity and amended § 312.10's prohibition against retaining such personal information for longer than is reasonably necessary for the specific purpose for which it is collected.

c. The Commission Amends § 312.10

After carefully considering the record and comments, and for the reasons stated in Part II.G.b, the Commission finalizes the amendments to § 312.10 that it proposed in the 2024 NPRM with minor modifications. In particular, the Commission is dropping the words "and not for a secondary purpose" from the first sentence of proposed § 312.10, and changing "purpose" to "purposes" in the second sentence of proposed § 312.10. The Commission is also removing the words "that precludes indefinite retention" from the fourth sentence of proposed § 312.10 because the third sentence of proposed § 312.10 states unequivocally that personal information collected online from a child may not be retained indefinitely. In addition, the Commission is changing "children's data retention policy" in proposed § 312.10 to "data retention policy," and inserting "addressing personal information collected from children" in the final sentence of proposed § 312.10 so that the revised sentence will state that "[t]he operator must provide the written data retention policy addressing personal information collected from children in the notice on its website or online service provided in accordance with § 312.4(d)." These changes make clearer that operators may only retain children's personal information for as long as reasonably necessary to fulfill the specific purposes for which it was collected, and that the amended Rule will not require an operator to establish, implement, and maintain a separate written children's data retention policy if the operator has established, implemented, and maintained a written data retention policy that encompasses children's personal information and meets the requirements the Commission proposed in § 312.10 of the 2024 NPRM.

H. Section 312.11: Safe Harbor Programs

Section 312.11 of the COPPA Rule enables industry groups or others to submit for Commission approval self-regulatory guidelines that implement substantially the same or greater protections for children as those contained in §§ 312.2 through 312.8 and 312.10 of the Rule. The provision requires FTC-approved COPPA Safe Harbor programs to satisfy specific obligations, including implementing an "effective, mandatory mechanism for the independent assessment" of member operators,[600] maintaining a protocol for disciplinary action,[601] and submitting to the FTC an annual report with "an aggregated summary of the results of the independent assessments."[602] In the 2024 NPRM, the Commission proposed several amendments to § 312.11 to enhance oversight of, and transparency regarding, FTC-approved COPPA Safe Harbor programs.

1. Proposal Related to § 312.11(b)(2)

a. The Commission's Proposal Regarding § 312.11(b)(2)

Section 312.11(b) requires FTC-approved COPPA Safe Harbor programs to demonstrate that they meet certain performance standards, including conducting an at least annual independent assessment of member operators' compliance with the Safe Harbor programs' self-regulatory program guidelines. Section 312.11(b)(2) currently specifies that a FTC-approved COPPA Safe Harbor program's required assessments of a member's compliance with the Safe Harbor program's guidelines must include comprehensive review of the member's "information policies, practices, and representations." In conjunction with the proposal to add more specificity to § 312.8 of the Rule, the 2024 NPRM proposed clarifying in § 312.11(b)(2) that

[600] 16 CFR 312.11(b)(2).
[601] 16 CFR 312.11(b)(3).
[602] 16 CFR 312.11(d)(1).

such comprehensive reviews must include member operators' "information privacy and security policies, practices, and representations."[603]

b. Public Comments Received in Response to the Commission's Proposal Regarding § 312.11(b)(2)

Several commenters expressed overall support for this proposed amendment to § 312.11(b)(2).[604] CARU noted that it "has been conducting a comprehensive review of member operators' information privacy and security policies, practices, and representations for over 20 years and welcomes" the Commission's proposed clarification regarding the required scope of annual assessments.[605] Another commenter supporting the proposed amendment suggested additionally requiring an independent assessment of the platform on which the operator hosts its service before the FTC-approved COPPA Safe Harbor program certifies the operator.[606]

Another commenter expressed support and suggested that, to the extent the revised COPPA Rule permits operators to comply with § 312.8 by maintaining a single comprehensive information security program that applies to the operator's business as a whole, rather than requiring a separate security program if one part of the operator's business is directed to children, then, consistent with that approach, the FTC-approved COPPA Safe Harbor programs should not require a separate children's personal information security program.[607]

---

[603] In the portion of the 2024 NPRM that set forth the proposed revised text of the COPPA Rule, the Commission inadvertently excluded what is currently—and what will remain in the revised COPPA Rule—the final sentence of § 312.11(b)(2). That sentence states: "The assessment mechanism required under this paragraph can be provided by an independent enforcement program, such as a seal program." The 2024 NPRM did not discuss or request comment on a proposal to remove that sentence for § 312.11(b)(2) because the Commission did not intend to make such a proposal.

[604] CARU, at 6; PRIVO at 6; CIPL, at 17.

[605] CARU, at 6.

[606] Truth in Advertising, Inc., at 15.

[607] CIPL, at 17. As discussed in Part II.F.b, the revised Rule permits operators to maintain a single comprehensive information security program that applies both to children's personal information and other information and otherwise meets § 312.8's requirements.

Some FTC-approved COPPA Safe Harbor programs expressed concerns about the proposed amendment of § 312.11(b)(2).[608] kidSAFE asserted that the proposed requirement for FTC-approved COPPA Safe Harbor programs to conduct a comprehensive review of an operator's information privacy and security program would exceed the competency of the Safe Harbor programs and require the programs to employ greater resources.[609] kidSAFE stated the cost of these additional resources would cause the FTC-approved COPPA Safe Harbor programs to significantly increase their fees, and suggested that the proposed amendment should therefore apply only to "larger entities."[610] Another FTC-approved COPPA Safe Harbor program, the Entertainment Software Rating Board (ESRB"), expressed concern that the proposal does not provide sufficient clarity regarding the Safe Harbor programs' "enhanced responsibilities," suggested that the proposal requires the programs to become "data security system auditors," and recommended either removing the security provision or providing more guidance.[611]

c. The Commission Amends § 312.11(b)(2)

After carefully considering the record and comments, the Commission is adopting the proposed amendment to § 312.11(b)(2). The Rule has always included both privacy- and security-related requirements, and the Commission in this rulemaking is putting more focus on operators' data security requirements. Revised § 312.11(b)(2) does not require operators to create an additional information security program exclusively dedicated to children's data. In parallel with adding specificity to the Rule's data security requirements,[612] the Commission expressly proposed that FTC-approved COPPA Safe Harbor programs' oversight of their

[608] kidSAFE, at 14; ESRB, at 14-15.
[609] kidSAFE, at 14.
[610] *Id.*
[611] ESRB, at 14-15.
[612] *See supra* Part II.F.

member operators must encompass both the privacy and security aspects of the Rule. Moreover, because an operator's overall security program may vary based on the operator's size, complexity, and nature and scope of activities, the cost and resources required to assess different operators' programs also may vary. Thus, the Commission would expect that small operators' practices might be significantly less expensive to review than the practices of larger operators. In fact, as noted earlier, one FTC-approved COPPA Safe Harbor program's comment pointed out that it already takes steps to assess operators' security practices to determine whether operators comply with current § 312.8.[613] Taking all those factors into consideration, the Commission disagrees that requiring FTC-approved COPPA Safe Harbor programs to review operators' security practices as well as privacy practices will impose undue burdens or make COPPA Safe Harbor program membership inaccessible.

2. Proposals Related to § 312.11(d)

Section 312.11(d) of the Rule sets forth requirements for FTC-approved COPPA Safe Harbor programs to, among other things, submit annual reports to the Commission and maintain for not less than three years, and make available to the Commission upon request, consumer complaints alleging that subject operators violated the Safe Harbor program's FTC-approved guidelines, records of the Safe Harbor program's disciplinary actions taken against subject operators, and results of the Safe Harbor program's § 312.11(b)(2) assessments.

To strengthen the Commission's oversight of FTC-approved COPPA Safe Harbor programs, the 2024 NPRM proposed several amendments to § 312.11(d). The Commission proposed to require FTC-approved COPPA Safe Harbor programs' mandatory reports to the Commission to (1) identify (a) each subject operator, (b) all approved websites or online

[613] CARU, at 6.

services, and (c) any subject operators that have left the safe harbor program, and (2) include (a) "a narrative description of the safe harbor program's business model," (b) "copies of each consumer complaint related to each subject operator's violation of [the] safe harbor program's guidelines," and (c) "a description of the process for determining whether a subject operator is subject to discipline."[614] The Commission also proposed to require each FTC-approved COPPA Safe Harbor program to publicly post a list of its subject operators on its websites or online services.[615] These amendments are intended to increase transparency. Each proposal is addressed in turn *infra*.

a. General Feedback Related to the Proposed Amendments to § 312.11(d)

One FTC-approved COPPA Safe Harbor program, iKeepSafe, expressed overall support for increased transparency in the Rule, stating that "the ability to monitor ongoing activities within all Safe Harbors would foster the ability to identify ongoing challenges within the Program or perhaps identify data privacy trends that can be addressed across the board."[616] Another commenter expressed general support for "the Commission's decision to increase transparency into safe harbor programs and promote accountability [for Safe Harbor programs]."[617]

Some commenters expressed concerns about the burden of the proposed additional reporting requirements.[618] One of those commenters suggested that FTC-approved COPPA Safe

[614] 89 FR 2034 at 2063-64.
[615] *Id.* at 2064.
[616] iKeepSafe, at 2-3.
[617] Advanced Education Research and Development Fund, at 8-9; *see also* Student Political Research Institute for New Governance, at 4-5 (encouraging the Commission to "take a more proactive role in monitoring Safe Harbor organizations' commitment to overseeing member compliance with children's privacy laws" and stating that the Commission should "encourage more independent organizations to submit a Safe Harbor application").
[618] Engine, at 3; The Toy Association, at 8-9.

Harbor programs would increase their membership fees as a result of having to comply with the reporting requirements as proposed and, consequently, that "[l]ow resourced companies, like startups," would leave their respective Safe Harbor programs.[619] Another commenter expressed concerns that the proposed amendments, if finalized, "will undermine the safe harbor process . . . [and] set new requirements that could be unduly burdensome for safe harbor programs to maintain and may discourage the scope of [safe harbor] participation that Congress expressly encouraged when enacting COPPA."[620]

The Commission takes seriously concerns about the burden and accessibility of COPPA Safe Harbor program membership as it balances the interests of consumers with the obligations placed on FTC-approved Safe Harbor programs and their members. But transparency and accountability of the FTC-approved COPPA Safe Harbor programs are important to encouraging COPPA compliance. The Commission believes that the proposed amendments to § 312.11(d) will impose modest or trivial costs (for example, in publicly identifying members).

Finally, one commenter recommended that the Commission require FTC-approved COPPA Safe Harbor programs' annual assessments of subject operators' compliance with Safe Harbor programs guidelines to be "publicly accessible."[621] The commenter opined that making the annual assessments publicly accessible would help parents make informed decisions and motivate operators to join the most protective Safe Harbor programs.[622]

While the Commission strongly agrees that helping parents make informed decisions is an important goal of the Rule, FTC-approved COPPA Safe Harbor programs' assessments of subject operators' compliance with their guidelines may include confidential and proprietary

[619] Engine, at 3.
[620] The Toy Association, at 8.
[621] Public Knowledge, at 7.
[622] *Id.*

information, as well as information about issues other than subject operators' compliance with the Safe Harbor program's guidelines. As discussed in further detail *infra*, a public assessment process could also have the perverse result of deterring FTC-approved COPPA Safe Harbor programs from identifying situations where operators need to remedy problems or from pushing for best practices in their assessments. For these reasons, the Commission declines to require Safe Harbors to publish their assessments of member operators.

i) Proposed Amendment to § 312.11(d)(1)

The 2024 NPRM proposed amending § 312.11(d)(1) to require FTC-approved COPPA Safe Harbor programs' annual reports to the Commission to identify each subject operator and all approved websites or online services, as well as any subject operators that left the program during the time period covered by the annual report. Commenters generally supported this proposed amendment to the annual report requirements.[623]

Some FTC-approved COPPA Safe Harbor programs expressed support for the proposed amendment.[624] One such commenter said that it "records, maintains and publishes each operator and its approved services publicly and in its annual report to the FTC and welcomes the inclusion of such requirements to ensure all safe harbors do the same."[625] After carefully considering the record and comments, and given the general support for the proposed amendment, the Commission adopts it as originally proposed.

ii) Proposed Amendment to § 312.11(d)(1)(i):

The Commission proposed to amend § 312.11(d)(1)(i) to require an FTC-approved COPPA Safe Harbor program's annual report to include a "narrative description of the Safe

[623] *See, e.g.*, CIPL, at 17-18; Advanced Education Research and Development Fund, at 8-9; iKeepSafe, at 2-3; ESRB, at 7; PRIVO, at 6; kidSAFE, at 15; Public Knowledge, at 3-6.
[624] *See* ESRB, at 7; iKeepSafe, at 2-3; PRIVO, at 6; kidSAFE, at 15.
[625] PRIVO, at 6-7; *see also* kidSAFE, at 15.

Harbor program's business model, including whether [the Safe Harbor program] provides additional services such as training to subject operators."

Most commenters that addressed this proposed amendment supported it. One FTC-approved COPPA Safe Harbor program noted that the Commission already collects a business model narrative in Safe Harbor programs' annual reports even though the Rule does not explicitly require it.[626] Another commenter suggested that this proposed amendment would enhance the Commission's oversight and help "identify potential conflicts early."[627] After carefully considering the record and comments, the Commission will amend the provision as proposed in the 2024 NPRM.

iii) Proposed Amendment to § 312.11(d)(1)(ii)

The Commission proposed to amend § 312.11(d)(1)(ii) to require FTC-approved COPPA Safe Harbor programs to submit with the Safe Harbor program's annual report to the Commission copies of each consumer complaint related to each subject operator's violation of the Safe Harbor program's guidelines. One FTC-approved COPPA Safe Harbor program supported this proposed amendment, but pointed out that Safe Harbor programs "do not necessarily have custody or control over consumer complaints related to each subject operator's violation of an FTC-approved COPPA Safe Harbor program's guidelines" unless they are directly provided to the Safe Harbor programs.[628] Another FTC-approved COPPA Safe Harbor program noted that most complaints received by operators are related to customer service issues (log in, functionality, *etc.*), and are not related to potential violations of the Safe Harbor program's guidelines.[629]

[626] ESRB, at 7-9.
[627] Public Knowledge, at 6.
[628] CARU, at 6.
[629] ESRB, at 7-9.

The Commission has carefully considered these points and does not seek to create a new requirement that FTC-approved COPPA Safe Harbor programs must collect complaints from operators. The proposed amendment requires FTC-approved COPPA Safe Harbor programs to submit consumer complaints that they receive directly or that an operator shares with the Safe Harbor program, but does not impose an additional obligation for a Safe Harbor program to request complaints from its member operators. After carefully considering the record and comments, the Commission amends § 312.11(d)(1)(ii) as originally proposed.

iv) Proposed Amendment to § 312.11(d)(1)(iv)

Current § 312.11(d)(1)(iii) requires that FTC-approved COPPA Safe Harbor programs' annual reports to the Commission include a description of any disciplinary action taken against any subject operator under § 312.11(b)(3). In the 2024 NPRM, the Commission proposed amending this provision, which, upon finalization of the proposed amendments, will now be redesignated as § 312.11(d)(1)(iv), to clarify that an FTC-approved COPPA Safe Harbor program's report must include a description of each disciplinary action the Safe Harbor program took against any subject operator during the reporting period and to require that the report include a description of the process for determining whether a subject operator was subjected to discipline.

One supportive commenter, Public Knowledge, stated that, along with the proposed requirement for FTC-approved COPPA Safe Harbor programs to include copies of consumer complaints related to violations of COPPA in their annual reports to the Commission, this proposed amendment "would strengthen internal regulation, empower parents to make informed decisions, and not significantly burden [Safe Harbor] programs."[630]

[630] Public Knowledge, at 3, 6.

Expressing concerns about this proposal, FTC-approved COPPA Safe Harbor program ESRB requested that the Commission clarify the proposed reporting requirement would apply only "to the formal disciplinary measures set out in Section 312.11(b)(3) of the COPPA Rule," and not require reporting on issues of non-compliance that do not lead to such disciplinary measures because the issues are, for example, technical and inadvertent and promptly and easily remediated.[631] The ESRB contended that the Commission should not hold FTC-approved COPPA Safe Harbor programs and their subject members to a "perfection" standard and stated that requiring a Safe Harbor program "to disclose every remedial action . . . would be self-defeating and dissuade companies from joining Safe Harbor programs."[632]

As the ESRB noted in its comment, the Commission's template for FTC-approved COPPA Safe Harbor program annual reports already asks programs to describe what constitutes a violation of the Safe Harbor program's guidelines and the types of disciplinary measures taken.[633] The Commission agrees that FTC-approved COPPA Safe Harbor programs should not hold subject operators to a standard of "perfection" and that it may sometimes be appropriate for Safe Harbor programs to take remedial actions other than disciplinary action under § 312.11(b)(3).

If an FTC-approved COPPA Safe Harbor program determines, in its assessment of an operator, that some corrective action is warranted but does not discipline the operator due to prompt responsiveness or other similar reasons, then amended § 312.11(d) will not require disclosure in the Safe Harbor program's annual report. In other words, the Commission is not attempting to redefine what constitutes a disciplinary action for subject operators' non-

[631] ESRB, at 9-10.
[632] *Id.* at 9.
[633] *Id.*

compliance with an FTC-approved COPPA Safe Harbor program's guidelines. After carefully considering the record and comments, the Commission is finalizing § 312.11(d)(1)(iv) as proposed.

v) Proposed Amendment to § 312.11(d)(4)

In the 2024 NPRM, the Commission also proposed amending § 312.11(d)(4) to require each FTC-approved COPPA Safe Harbor program to "publicly post a list of all current subject operators on [its] websites and online services," and to "update the list every six months to reflect any changes to the approved safe harbor program['s] subject operators or their applicable websites and online services."[634]

Some commenters supported the proposal to require FTC-approved COPPA Safe Harbor programs to publicly identify members, including those who leave the Safe Harbor program.[635] One such commenter highlighted, for example, that the proposal (along with other proposed amendments to § 312.11) would bolster parents' ability to make informed decisions, "strengthen internal regulation, empower parents to make informed decisions, and not significantly burden programs, as they already should submit annual reports and maintain up-to-date lists of their operators."[636]

By contrast, some commenters expressed concerns about the proposal to require FTC-approved COPPA Safe Harbor programs to publicly identify members..[637] The ESRB warned that implementation of the proposed requirement could mislead consumers "into believing that all products and services provided by the company have been certified as compliant by the Safe

[634] 89 FR 2034 at 2076.
[635] PRIVO, at 6; CIPL, at 18.
[636] Public Knowledge, at 6.
[637] ESRB, at 10-11; kidSAFE, at 15-16; ANA, at 17.

Harbor" program.[638] kidSAFE supported a requirement for Safe Harbor programs to post member lists publicly subject to the "very important condition" that the Commission limit the requirement to certified products and not include operators or products that are under review for potential certification.[639] In response to these comments, the Commission clarifies that the requirement to identify certified products or services applies to those that have been approved, not those that are under review for possible certification.

The Commission expects that FTC-approved COPPA Safe Harbor programs' identification of members will be helpful to parents as they make decisions about which websites or online services to allow their children to use. A number of FTC-approved COPPA Safe Harbor programs already identify their members in various ways, such as on their websites or by having members display seals indicating their participation in the program.[640] The Commission believes that parents rely on these indicia of participation and place confidence in a certified product's or service's COPPA compliance. However, in order to address the issue FTC-approved COPPA Safe Harbor programs raised with respect to certifications that apply only to a particular product or service offered by a member that also offers other products or services that are not certified, the Commission adopts the proposed amendments to § 312.11(d)(4) with minor modifications. The Commission's intent for this provision is to require FTC-approved COPPA Safe Harbor programs to publicly share a list of the particular websites and online services

[638] ESRB, at 10.
[639] kidSAFE, at 15-16.
[640] Some commenters suggested that standardization of the FTC-approved COPPA Safe Harbor programs' seals would help clarify to parents what the seal and certification signify. *See* Public Knowledge, at 5, 7-8; ESRB, at 11-12; *see also* Truth in Advertising, Inc., at 9-13 (suggesting the Commission address when and how Safe Harbor certification seals may be used to prevent deceptive representations). One such commenter referenced the fact that FTC-approved COPPA Safe Harbor programs may offer various certifications and seals related to, for example, assessment of privacy practices unrelated to COPPA or the FTC-approved guidelines. ESRB, at 4. The Commission believes that the amendments it is adopting will make it easier for parents to determine whether websites or online services are participants in an FTC-approved COPPA Safe Harbor program without being overly prescriptive about how Safe Harbor programs organize their websites and other communications.

certified by their respective programs. If there is a version of a particular service, for example, that is certified only for one operating system but not for another, the list must reflect that limitation. With this in mind, amended § 312.11(d)(4) states that FTC-approved COPPA Safe Harbor programs shall "publicly post on each of the approved safe harbor program's websites and online services a list of all current subject operators and, for each such operator, list each certified website or online service."

3. Proposed § 312.11(f)

The Commission proposed that FTC-approved COPPA Safe Harbor programs submit triennial reports detailing each Safe Harbor program's technological capabilities and mechanisms for assessing members' fitness for membership in each respective program. The Commission received several comments in support of this proposed amendment.[641] One commenter that supported the proposal suggested the Commission should also set out minimum expectations for such benchmarks.[642]

Because the technologies that FTC-approved COPPA Safe Harbor programs use to assess operators' practices may change as business practices change and as the tools used to assess those practices evolve, the Commission declines to set forth such standards in the Rule. In the process of reviewing the triennial reports and annual reports, the Commission expects that agency staff will raise concerns if the technical tools employed are inadequate.

4. Proposed § 312.11(g)

Current § 312.11(f) 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, and requires modifications to Safe Harbor guidelines

[641] CIPL, at 17-18; NAI, at 7; PRIVO, at 7.
[642] ESRB, at 12.

to be submitted prior to March 1, 2013. The Commission proposed to redesignate this provision as § 312.11(g) in light of the newly proposed § 312.11(f), and to delete the March 2013 deadline because this date has long passed.

Several comments supported the proposed amendments to this section.[643] Relatedly, in addressing § 312.11(g), kidSAFE recommended that, after the final Rule at issue is published, the Commission provide Safe Harbor programs at least six months to submit revised guidelines for approval and another six months to implement the new guidelines to measure members' compliance.[644] Other FTC-approved COPPA Safe Harbor programs also made similar recommendations.[645] The Commission agrees that FTC-approved COPPA Safe Harbor programs will need time to assess the revisions to the Rule and revise their guidelines and practices to reflect the changes. After carefully considering the record and comments, the Commission will revise § 312.11(g) to state that FTC-approved COPPA Safe Harbor programs shall submit proposed modifications to their guidelines within six months after the final Rule is published in the *Federal Register*.

5. Proposed § 312.11(h)

Current § 312.11(g) addresses operator compliance with the FTC-approved COPPA Safe Harbor program guidelines. In the 2024 NPRM, the Commission proposed to redesignate this provision as § 312.11(h) in light of its proposal to add a new paragraph (f) in § 312.11 and the resulting need to redesignate paragraph (g) in § 312.11. The Commission did not receive any comments related to this proposed amendment and will therefore adopt it as originally proposed.

[643] CIPL, at 18; ESRB, at 25-26; CARU, at 7.
[644] kidSAFE, at 16.
[645] ESRB, at 25-26 (requesting "at least a six month deadline" to submit revised program guidelines to the Commission for approval); CARU, at 7 (recommending a period of at least one year for operators to come into complete compliance with the final Rule).

6. NPRM Question Nineteen: Safe Harbor Program Conflicts of Interest

In the 2024 NPRM, the Commission solicited comments on what conflicts would affect an FTC-approved COPPA Safe Harbor program's ability to effectively assess a subject operator's fitness for membership.[646]

The Commission received few comments addressing this issue. One commenter raised concerns that FTC-approved COPPA Safe Harbor programs may offer compliance consulting services in addition to their role in overseeing member operators' compliance with the guidelines, and that such a dual role is a conflict of interest.[647] Another posited that there is a "natural conflict" inherent in the Safe Harbor concept because approved programs have incentive to have more members.[648] Another commenter questioned whether advertising platforms can be adequately assessed by FTC-approved COPPA Safe Harbor programs.[649]

The Commission received responses from two FTC-approved COPPA Safe Harbor programs regarding conflicts of interest. The ESRB rejected "the assumption that conflicts of interest are inherent in the COPPA Safe Harbor program," pointing among other things to the Commission's "robust" oversight of the Safe Harbor programs.[650] CARU indicated that it does not require companies to contribute financially to its organization other than the fee for the review service and does not require members to purchase other products or services, to avoid conflicts of interest.[651]

---

[646] 89 FR 2034 at 2071 (Question 19).
[647] Public Knowledge, at 2.
[648] Internet Safety Labs, at 11
[649] *Id.* at 11-12.
[650] ESRB, at 16-18. The ESRB indicated that while it does not provide COPPA consulting services, it would not recommend prohibiting FTC-approved COPPA Safe Harbor programs from doing so, albeit potentially subject to additional transparency requirements. *Id*. at 18.
[651] CARU, at 6-7.

Based on the comments received, the Commission has determined that the proposed amendments to FTC-approved COPPA Safe Harbor reporting requirements under the Rule will facilitate the Commission's ability to monitor Safe Harbor programs and that it is unnecessary to adopt additional amendments to the Rule to address potential conflicts of interest. The Commission will continue to monitor the FTC-approved COPPA Safe Harbor programs closely.

I. Other Issues

1. NPRM Question Two: Automatic Deletion of Information Collected

a. The Commission's Question Regarding Automatic Deletion of Information Collected

Currently, the Rule defines "[c]ollects or collection" as, in relevant part, "the gathering of any personal information from a child by any means, including … [e]nabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records."[652] During the Rule review that led to the 2013 Amendments, the Commission explained that movement from a 100% deletion standard to a "reasonable measures" standard would enable operators to implement automated filtering systems to delete personal information from children's postings.[653] In Question Two of the 2024 NPRM's "Questions for the Proposed Revisions to the Rule" section, however, the Commission stated its concern that, if automatic moderation or filtering technologies can be circumvented, reliance on them may not be appropriate in a context where a child is

[652] 16 CFR 312.2.
[653] *See* 78 FR 3972 at 3973-3974; 76 FR 59804 at 59808.

communicating one to one with another person privately instead of in a public posting.[654] Based on that concern, the Commission requested comment on whether the Commission should retain its position that an operator will not be deemed to have "collected" a child's personal information and therefore will not have to comply with the COPPA Rule's requirements if it employs automated means to delete personal information from one-to-one communications.[655]

b. Public Comments Received in Response to the Commission's Question Regarding Automatic Deletion of Information Collected

Overall, the Commission received relatively few comments in response to Question Two. Some commenters generally supported the Commission continuing to permit the use of automatic moderation or filtering technologies as a means to delete all or virtually all personal information from children's one-to-one communications.[656] One commenter asserted generally that permitting the use of automated filtering systems to enable an operator to avoid being deemed to have "collected" personal information from a child "aligns with the [COPPA] Rule's scope."[657]

Asserting that automated filtering entails holding data at least briefly in order to delete it, one commenter opposed the Commission continuing to permit the use of automated filtering systems as a means for operators to avoid being deemed to have collected personal information from children in any context, including one-to-one communications.[658] Another commenter asserted that "there is no way such automated means will work" and raised the possibility that

[654] *See* 89 FR 2034 at 2069 (Question 2).
[655] *Id.*
[656] SIIA, at 13-14; The Toy Association, at 4.
[657] M. Bleyleben, at 1. Like commenters that opposed the Commission permitting the use of automated filtering systems to enable an operator to avoid being deemed to have "collected" personal information from a child, this commenter acknowledged that deletion of personal information from communications "will necessarily require momentary processing of personal information."
[658] Parent Coalition for Student Privacy, at 10-11.

any deletion mechanism may have "bugs which result in leakage or misuse."[659] This commenter suggested that "any deletion requirement that is to be meaningful needs to specify particular timelines within which deletion must occur."[660] Another commenter raised the concern that monitoring one-on-one communication could impair encryption security.[661]

In all, commenters largely did not weigh in as to whether an operator should be allowed to enable a child to communicate one-to-one with another user, possibly an adult, without providing notice or seeking verifiable parental consent from the parent, when the one-to-one communication is moderated by the operator using automated means alone. That question concerns whether automated means are sufficiently reliable to ensure safety when a child is in direct communication with another individual (as opposed to a context where the communications will be available to other users, such as in a chat room).

c. The Commission Declines to Make Rule Amendments Related to NPRM Question Two

In reply to commenters' responses to Question Two of the "Questions for the Proposed Revisions to the Rule" section of the 2024 NPRM regarding deletion, the Commission expects that operators relying upon automatic deletion of children's personal information to avoid having to provide notice and obtain verifiable parental consent will ensure that such deletion occurs in real time, concurrent with facilitating the communication, and without storing the personal information for any length of time. The Commission does not propose to adopt changes to

[659] Internet Safety Labs, at 2.
[660] *Id.*
[661] ACLU, at 9 ("On one hand, the current Rule permits operators to remove children's personal information from one-to-one messaging, thus allowing known children and users of child-directed services to engage in additional forms of communication, speech, and learning. On the other hand, such measures likely require the monitoring of users' messages and may pose technical difficulties when implemented alongside privacy-protective measures such as end-to-end encryption."). The Commission notes that if an operator covered by the Rule enabled a child to communicate with others via end-to-end encryption, the operator would have to provide notice and obtain verifiable parental consent.

require notice and verifiable parental consent in this circumstance. However, the Commission will monitor this issue closely for potential abuse.

2. NPRM Question Twenty: Effective Date of Rule Amendments

a. The Commission's Question Regarding Effective Date of Rule Amendments

In the 2024 NPRM, the Commission requested comment on whether an effective date of six months after the issuance of the Commission's final Rule would be an appropriate effective date for any proposed changes that do not specify an effective date.[662] In so doing, the Commission noted that the Commission had taken the same approach with the issuance of the initial COPPA Rule and the 2013 Amendments.[663]

b. Public Comments Received in Response to the Commission's Question Regarding Effective Date of Rule Amendments

Most commenters that opined on an appropriate effective date recommended that the effective date be one year[664] or longer[665] after issuance of the final Rule. Such commenters asserted that the breadth or complexity of the proposed amendments weigh in favor of the

[662] 89 FR 2034 at 2071 (Question 20).
[663] *Id.*
[664] ESRB, at 25-26 (also requesting at least six months for FTC-approved COPPA Safe Harbor programs to submit their revised program guidelines to the FTC); kidSAFE, at 16; CARU, at 7; TechNet, at 6. *See also* NCTA, at 23 ("Depending on the changes the Commission ultimately adopts, operators may need to update their privacy disclosures, consent process, contracts with service providers, and data security policies and practices. Given that some operators have multiple websites and apps and work with many different service providers, a six-month implementation period is insufficient for significant changes to COPPA Rule requirements."); The Toy Association, at 9 (stating that a majority of the association's members are small businesses and that it would be difficult for them to meet a six-month compliance deadline; recommending a minimum of a one-year compliance deadline).
[665] ITIC, at 7 (recommending that the effective date be 18-24 months after issuance of the final Rule due to the breadth of the proposed amendments); Chamber, at 12 (recommending that the effective date be two years after publication of the final Rule "in line with Europe's General Data Protection Regulation"); IAB, at 27-28 (same); Consumer Technology Association, at 3 (same); Internet Infrastructure Coalition, at 4-5 (recommending that the effective date be up to two years after publication of the final amended rule to recognize and balance the compliance complexity among businesses of different sizes, resources, and breadth, and especially to help small- and medium-sized businesses); CCIA, at 11 (recommending providing 18-24 months for compliance because the proposed amendments would greatly expand the scope and extent of obligations).

effective date being more than six months after issuance of the final Rule. On the other hand, one commenter "strongly urge[d]" the Commission to implement the proposed amendments "in the shortest time frame possible" and opined that the proposed amendments are not significant enough to warrant the Commission making the effective date later than six months after issuance of the final Rule.[666] Another commenter stated that the Commission should set an effective date that "balance[s] the urgency of protecting children's privacy with the practical considerations of implementation for those affected by the changes, including comprehensive understanding, proper implementation, and adjustment by all stakeholders involved."[667]

c. The Commission Changes the Effective Date in Response to NPRM Question Twenty Comments

The Commission has carefully considered the record and comments regarding an appropriate effective date for any proposed changes that do not specify an effective date. The effective date for the final Rule will be 60 days from the date the final Rule is published in the *Federal Register*. In order to account for some of the commenters' concern that entities subject to the Rule will need more than six months after the Final Rule's publication to assess the Rule amendments and revise their policies and practices to comply with them, the final Rule provides 365 days from the final Rule's publication date to come into full compliance with the amendments that do not specify earlier compliance dates. The Commission clarifies that, during this 365-day period, regulated entities may comply with the Rule provisions that do not specify earlier compliance dates either by complying with the pre-2025 Rule or with the revised Rule. That said, the final Rule specifies earlier compliance dates related to obligations on FTC-approved COPPA Safe Harbor programs of six months after the Rule's publication date for

[666] M. Bleyleben, at 8.
[667] Yoti, at 17-18.

§ 312.11(d)(1), 90 days after the Rule's publication date for § 312.11(d)(4), and six months after the Rule's publication date for § 312.11(g).

III. Paperwork Reduction Act

The Paperwork Reduction Act ("PRA"), 44 U.S.C. chapter 35, requires federal agencies to seek and obtain approval from the Office of Management and Budget ("OMB") before undertaking a collection of information directed to ten or more persons.[668] Under the PRA, a rule creates a "collection of information" when ten or more persons are asked to report, provide, disclose, or record information in response to "identical questions."[669] The existing COPPA Rule contains recordkeeping, disclosure, and reporting requirements that constitute "information collection requirements" as defined by 5 CFR 1320.3(c) under the OMB regulations that implement the PRA. OMB has approved the Rule's existing information collection requirements through April 30, 2025 (OMB Control No. 3084–0117).[670] This final Rule modifies the collections of information in the existing COPPA Rule. For example, the amendments to the COPPA Rule adopted here amend the definition of "website or online service directed to children," potentially increasing the number of operators subject to the Rule, albeit likely not to a significant degree. FTC staff believes that any such increase will be offset by other operators of websites or online services adjusting their information collection practices so that they will not be subject to the Rule. The amendments also increase disclosure obligations for operators and FTC-approved COPPA Safe Harbor programs, and FTC-approved COPPA Safe Harbor programs will also face additional reporting obligations under the amended Rule.

[668] 44 U.S.C. 3502(3)(A)(i).
[669] *See* 44 U.S.C. 3502(3)(A).
[670] The 2024 NPRM erroneously indicated that the Rule's information collection requirements were approved through March 31, 2025.

While the amended Rule requires operators to establish, implement, and maintain a written comprehensive security program and data retention policy, such requirements do not constitute a "collection of information" under the PRA. Namely, under the amended Rule, each operator's security program and the safeguards instituted under such program will vary according to the operator's size and complexity, the nature and scope of its activities, and the sensitivity of the information involved. Thus, although each operator must summarize its compliance efforts in one or more written documents, the discretionary balancing of factors and circumstances that the amended Rule allows does not require entities to answer "identical questions" and therefore does not trigger the PRA's requirements.[671]

As required by the PRA, the Commission sought OMB review of the modified information collection requirements at the time of the publication of the NPRM. OMB directed the Commission to resubmit its request at the time the final Rule is published. Accordingly, simultaneously with the publication of this final Rule, the Commission is resubmitting its clearance request to OMB. FTC staff has estimated the burdens associated with the amendments as set forth below.

A. Practical Utility

[671] The IAB raised Paperwork Reduction Act issues with respect to the requirement that operators develop a written security program, and asked that the Commission 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." IAB, at 23-24. The Commission has made a change in the final Rule to make clear that an operator is not required to implement requirements specifically to protect the confidentiality, security, and integrity of personal information collected from children if the operator has established, implemented, and maintained an information security program that applies both to children's personal information and other information and otherwise meets the requirements the Commission had proposed in § 312.8 of the 2024 NPRM.

According to the PRA, "practical utility" is "the ability of an agency to use information, particularly the capability to process such information in a timely and useful fashion."[672] The Commission has maximized the practical utility of the new disclosure (notice) and reporting requirements contained in the final Rule amendments, consistent with the requirements of COPPA.

With respect to disclosure requirements, the amendments to § 312.4(c) more clearly articulate the specific information that operators' direct and online notices for parents must include about their information collection and use practices, and ensure that parents have the information that they need to assess the operator's practices and determine whether to grant consent. For example, the Rule previously required that operators retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose(s) for which the information was collected; the revised Rule requires each operator to set down its retention policy in writing and to disclose that policy to parents in the online notice. Similarly, the amended Rule will require operators that disclose personal information to third parties to state in the direct notice the identities or specific categories of such third parties;[673] the purposes for such disclosure; and that the parent can consent to the collection and use of the child's personal information without consenting to the disclosure of such personal information to third parties for non-integral purposes. This disclosure requirement provides parents with information about the purpose for and scale of disclosure to third parties and effectuates the parental right, in effect since the Rule was originally promulgated, to object to certain third-party disclosures. The

[672] 44 U.S.C. 3502(11). In determining whether information will have "practical utility," OMB will consider "whether the agency demonstrates actual timely use for the information either to carry out its functions or make it available to third-parties or the public, either directly or by means of a third-party or public posting, notification, labeling, or similar disclosure requirement, for the use of persons who have an interest in entities or transactions over which the agency has jurisdiction." 5 CFR 1320.3(l).

[673] The operator must disclose both the names and the categories of third parties in its online notice.

amended Rule also formally adopts an exception, previously reflected in a discretionary enforcement policy, that allows operators to collect audio files in certain circumstances when the operator describes in its online notice how the operator uses such audio files. The Rule also requires the small number of FTC-approved COPPA Safe Harbor programs to publicly post lists of each subject operator's certified websites and online services (which the programs already maintain as part of their normal business operations). These modifications are intended to increase transparency and enable parents and the public to determine whether a particular website or online service has been certified by an approved Safe Harbor program.

With respect to reporting obligations, the amended Rule includes additional reporting obligations that will apply only to the small number of FTC-approved Safe Harbor programs. The changes include additional requirements for Safe Harbor programs' mandatory reports to the Commission to identify each subject operator and their approved websites or online services, as well as any subject operators that have left the Safe Harbor program; describe the Safe Harbor program's business model; describe the process for determining whether an operator is subject to discipline; and provide copies of consumer complaints related to each subject operator's violation of the program's guidelines.[674] These requirements strengthen the FTC's oversight of FTC-approved COPPA Safe Harbor programs by providing the agency with information to assess whether operators participating in the programs may be violating the Rule, and make the FTC's own oversight more transparent to the public.

[674] The ESRB indicated that it receives "very few complaints that are actually about companies' privacy practices" so the requirement to provide complaints is not "necessary for the proper performance of the functions of the FTC" nor will it have "practical utility" as required by the Paperwork Reduction Act. ESRB, at 9 (internal quotation marks omitted). However, the amended Rule provision requires approved Safe Harbor program to provide "copies of each consumer complaint *related to each subject operator's violation of a safe harbor program's guidelines*." (emphasis added). The amended Rule thus does not require Safe Harbor programs to provide complaints that are not germane to companies' privacy practices.

Given the justifications stated above for the amended disclosure and reporting requirements, the amendments will have significant practical utility.[675]

B. Explanation of Estimated Incremental Burden Under the Amendments

1. Number of Respondents

As noted in the Regulatory Flexibility Act section, FTC staff estimates that in 2025 there are approximately 6,140 operators subject to the Rule.[676] FTC staff does not believe that the amendments to the Rule's definitions will affect the number of operators subject to the Rule. For example, FTC staff does not expect that the Commission's addition of "biometric identifiers" to the Rule's definition of "personal information" will significantly alter the number of operators subject to the Rule. FTC staff believes that all or nearly all operators of websites or online services that collect "biometric identifiers" from children are already subject to the Rule. In total, to the extent that any of the Commission's amendments to the Rule's definitions might result in minor additional numbers of operators being subject to the Rule, FTC staff believes that any such increase will be offset by other operators of websites or online services adjusting their information collection practices so that they will not be subject to the Rule.

For this burden analysis, FTC staff updates its recently published estimate to 430 new operators per year.[677] Commission staff retains its estimate that no more than one additional

---

[675] The Commission has also declined to adopt certain potential changes to the Rule on the basis of potential burden or lack of utility. For example, the Commission has not amended the Rule to provide an exemption for an operator that undertakes an analysis of its audience composition and determines that no more than a specific percentage of its users are likely to be children under 13. *See* IAB, at 15 (addressing Question 11 of the "Questions for the Proposed Revisions to the Rule" section of the 2024 NPRM by raising burden objections, in particular with respect to use of such technology by small- and medium-sized businesses).

[676] This estimate differs from the number of operators subject to the COPPA Rule estimated in the 2024 NPRM, 5,710. *See* 2024 NPRM, 89 FR 2034 at 2065. That estimate has been updated for 2025 by adding an estimated 430 new operators for the past year. This leads to the current estimated number of 6,140 operators subject to the Rule (5,710 + 430= 6,140).

[677] The average growth rate from 2013 through 2021 for Software Publishing and Other Information Services (which includes Internet publishing) was 7.4%. *See* https://www.census.gov/programs-surveys/susb/data/tables.html. Multiplying this rate by the estimated number of existing operators, 5,710, gives an estimate of approximately 430

entity will become an FTC-approved COPPA Safe Harbor program within the next three years of PRA clearance.

2. Recordkeeping Hours

Commission staff does not expect that the Rule amendments will increase operators' recordkeeping obligations. With respect to the FTC-approved COPPA Safe Harbor programs, similarly, the Commission has not revised the recordkeeping requirement applicable to those programs under § 312.11(d)(3).

3. Disclosure Hours

a. New Operators' Disclosure Burden

Based on Census data, FTC staff estimates that the Rule affects approximately 430 new operators per year. FTC staff does not expect that new operators' obligations with respect to disclosure of their privacy practices through a direct notice and an online notice will take more time to complete under the revised Rule than under the existing Rule, except with respect to disclosure of a data retention policy. The amended Rule includes a new requirement that operators disclose a data retention policy. Commission staff estimates it will require, on average, approximately 10 hours to meet the data retention policy requirement.[678] This yields an estimated incremental annual hours burden of 4,300 hours (430 respondents × 10 hours).

---

new operators per year on a going forward basis. This new estimate is different from the previously published estimate of 280 new operators per year in the 2024 NPRM as it uses a different, more up-to-date data source. *See* 2024 NPRM, 89 FR 2034 at 2065 n.354.

[678] As discussed in Part II.G.b, the IAB asserted that this 10-hour estimate is low and also requested that the Commission clarify that an existing retention policy that is compliant with the requirements in the Rule is sufficient. *See* IAB, at 21, 23. A retention policy that complies with the requirements in the Rule is adequate even if the policy were adopted before the revised Rule was promulgated. With respect to the estimated burden hours, the comments received as a whole do not support the view that the estimate is low. The Commission believes that the requirement that operators' written data retention policies state the purposes for which children's personal information is collected, the business need for retaining such information, and the timeframe for deleting it will require no more than approximately 10 hours per operator because, to comply with the existing COPPA Rule and other laws and regulations and for operational reasons, the Commission believes that many covered operators already have written data retention policies that include the same or largely the same elements that the Commission is now requiring in the amended Rule.

b. Existing Operators' Disclosure Burden

The amended Rule imposes various new disclosure requirements on operators that will require them to update the direct and online notices that they previously provided. Specifically, the amendments require operators to update the direct and online notices with additional information about the operators' information practices. Additionally, the amended Rule requires operators to disclose a data retention policy. Finally, the amended Rule will now require operators utilizing the support for the internal operations exception, 16 CFR 312.5(c)(7), to provide an online notice.[679]

FTC staff believes that an existing operator's time to make these changes to its online and direct notices for the first time would be no more than that estimated for a new entrant to craft an online notice and direct notice for the first time, *i.e.,* 60 hours.[680] Additionally, as discussed previously, FTC staff believes the time necessary to develop, draft, and publish a data retention policy is approximately 10 hours. Therefore, these disclosure requirements will amount to a one-time burden of approximately 70 hours. Annualized over three years of PRA clearance, this amounts to approximately 23 hours (70 hours ÷ 3 years) per operator each year. Aggregated for the 6,140 existing operators, the annualized disclosure burden for these requirements would be approximately 141,220 hours per year (6,140 respondents × 23 hours).

[679] Previous burden estimates have not distinguished between the burden on this subset of operators who had no disclosure obligations under the Rule and the burden on operators who were required to provide both a direct and an online notice – the analysis assumed that this subset of operators had the same, higher burden. This analysis takes the same approach in assuming that operators who now have to provide an online notice will have the same burden, 60 hours, to develop an online notice as other existing operators would take to develop both a direct notice and an online notice.

[680] FTC staff maintains its longstanding estimate that new operators of websites and online services will require, on average, approximately 60 hours to draft a privacy policy, design mechanisms to provide the required online privacy notice, and, where applicable, provide the direct notice to parents. *See, e.g.*, Children's Online Privacy Protection Rule, Notice, 86 FR 55609 (Oct. 6, 2021), available at *https://www.govinfo.gov/app/details/FR-2021-10-06/2021-21753*; 2022 COPPA PRA Supporting Statement, available at https://omb.report/icr/202112-3084-002/doc/119087900.

The amended Rule will also require each FTC-approved COPPA Safe Harbor program to provide a list of all current subject operators, websites, and online services on each of the FTC-approved COPPA Safe Harbor program's websites and online services, and the amended Rule further requires that such list be updated every six months thereafter. Because FTC-approved COPPA Safe Harbor programs already keep up-to-date lists of their subject operators, FTC staff does not anticipate this requirement will significantly burden FTC-approved COPPA Safe Harbor programs. To account for time necessary to prepare the list for publication and to ensure that the list is updated every 6 months, FTC staff estimates 10 hours per year. Aggregated for one new FTC-approved COPPA Safe Harbor program and six existing FTC-approved COPPA Safe Harbor programs, this amounts to an estimated cumulative disclosure burden of 70 hours per year (7 respondents × 10 hours).

4. Reporting Hours

The amendments will require FTC-approved COPPA Safe Harbor programs to include additional content in their annual reports. The amendments will also require each FTC-approved COPPA Safe Harbor program to submit a report to the Commission every three years detailing the program's technological capabilities and mechanisms for assessing subject operators' fitness for membership in the program.

The burden of conducting subject operator audits and preparing the annual reports likely varies by FTC-approved COPPA Safe Harbor program, depending on the number of subject operators. FTC staff estimates that the additional reporting requirements for the annual report will require approximately 50 hours per program per year. Aggregated for one new FTC-approved COPPA Safe Harbor program (50 hours) and six existing FTC-approved COPPA Safe

Harbor programs (300 hours), this amounts to an estimated cumulative reporting burden of 350 hours per year (7 respondents × 50 hours).

Regarding the reports that the amended Rule will require FTC-approved Safe Harbor programs to submit to the Commission every three years, § 312.11(c)(1) of the existing Rule already requires FTC-approved COPPA Safe Harbor programs to include similar information in their initial application to the Commission. Specifically, existing § 312.11(c)(1) requires that the application address FTC-approved COPPA Safe Harbor programs' business models and the technological capabilities and mechanisms they will use for initial and continuing assessment of operators' fitness for membership in their programs. Consequently, the three-year reports should merely require reviewing and potentially updating an already-existing report. FTC staff estimates that reviewing and updating existing information to comply with amended § 312.11(f) will require approximately 10 hours per FTC-approved COPPA Safe Harbor program. Divided over the three-year period, FTC staff estimates that annualized burden attributable to this requirement would be approximately 3.33 hours per year (10 hours ÷ 3 years) per FTC-approved COPPA Safe Harbor program, which staff will round down to 3 hours per year per FTC-approved COPPA Safe Harbor program. Given that several FTC-approved COPPA Safe Harbor programs are already available to website and online service operators, Commission staff anticipates that no more than one additional entity is likely to become an FTC-approved COPPA Safe Harbor program within the next three years of PRA clearance. Aggregated for one new FTC-approved COPPA Safe Harbor program and six existing FTC-approved COPPA Safe Harbor programs, this amounts to an estimated cumulative reporting burden of 21 hours per year (7 respondents × 3 hours).

5. Labor Costs

a. Disclosure

i New Operators

As previously noted, FTC staff estimates an incremental annual burden of 4,300 hours (430 respondents × 10 hours) associated with developing and posting a retention policy in the online notice. Consistent with its past estimates and based on its 2013 rulemaking record,[681] FTC staff estimates that the time spent on compliance for new operators covered by the COPPA Rule would be apportioned five to one between legal (outside counsel lawyers or similar professionals) and technical (*e.g.*, computer programmers, software developers, and information security analysts) personnel. Therefore, FTC staff estimates that approximately 3,583 of the estimated 4,300 hours required will be completed by legal staff.

Regarding legal personnel, FTC staff anticipates that the workload among law firm partners and associates for assisting with COPPA compliance would be distributed among attorneys at varying levels of seniority.[682] Assuming two-thirds of such work is done by junior associates at an estimated rate of approximately $559 per hour in 2025, and one-third by senior partners at an estimated rate of approximately $847 per hour in 2025, the weighted average of outside counsel costs would be approximately $655 per hour.[683]

---

[681] *See, e.g.*, 78 FR 3972 at 4007 (Jan. 17, 2013); 2022 COPPA PRA Supporting Statement, available at *https://omb.report/icr/202112-3084-002/doc/119087900*.

[682] For the purposes of this calculation, FTC staff considers a senior partner to have 12 or more years of experience and a junior attorney to have one or zero years of experience.

[683] These estimates are drawn from the "Fitzpatrick Matrix." The Fitzpatrick Matrix was developed to provide a tool for the "reliable assessment of fees charged for complex [civil] federal litigation," in the District of Columbia, and has been adopted by, among others, the Civil Division of the United States Attorney's Office for the District of Columbia. *See* Fitzpatrick Matrix, Civil Division of the United States Attorney's Office for the District of Columbia, Fitzpatrick Matrix, 2013–2024 (quoting *DL v. District of Columbia*, 924 F.3d 585, 595 (D.C. Cir. 2019)), available at *https://www.justice.gov/usao-dc/media/1353286/dl?inline*. It is used here as a proxy for market rates for litigation counsel in the Washington, DC area. In order to estimate what the mean hourly wages will be in 2025 ($559 and $847 for junior associates and senior partners), staff applies the average growth rate in wages from 2013 through 2024 for junior associates and senior partners (9.7% and 5.5% respectively) to the 2024 mean hourly wages ($510 and $803) for one additional year.

FTC staff anticipates that computer programmers responsible for posting privacy policies and implementing direct notices and parental consent mechanisms would account for the remaining 717 hours. FTC staff estimates an hourly wage of $60.43 for technical personnel in 2025, based on Bureau of Labor Statistics ("BLS") data.[684] Accordingly, associated annual labor costs would be $2,390,193 in 2025 [(3,583 hours × $655/hour) + (717 hours × $60.43/hour)] for the estimated 430 new operators.

ii. Existing Operators

As previously discussed, FTC staff estimates that the annualized disclosure burden for these requirements for the 6,140 existing operators would be 141,220 hours per year. Thus, apportioned five to one, this amounts to 117,683 hours of legal and 23,537 hours of technical assistance. Applying hourly rates of $655 and $60.43, respectively, for these personnel categories, associated labor costs would total approximately $78,504,706 ($77,082,365 + $1,422,341) in 2025.

iii. Safe Harbor Programs

Previously, industry sources have advised that all of the labor to comply with new Safe Harbor program requirements would be attributable to the efforts of in-house lawyers. FTC staff estimates an average hourly rate of $111.94 for a Washington D.C. in-house lawyer in 2025.[685] Applying this hourly labor cost estimate to the hours burden associated with the estimated 70-

[684] The estimated mean hourly wages for technical personnel ($56.03) are based on an average of the mean hourly wage for computer programmers, software developers, information security analysts, and web developers as reported by the Bureau of Labor Statistics. *See* Bureau of Labor Statistics, Occupational Employment and Wages—May 2023, Table 1 (May 2023) ("BLS Table 1"), available at *https://www.bls.gov/news.release/ocwage.t01.htm* (National employment and wage data from the Occupational Employment Statistics survey by occupation). In order to estimate what the mean hourly wages will be in 2025 ($60.43), staff applies the average growth rate in wages from 2013 through 2023 for technical personnel (3.85%) to the 2023 mean hourly wages ($56.03) for two additional years.

[685] *https://www.roberthalf.com/us/en/job-details/in-house-counselassociate-general-counsel-10-years-experience/washington-dc*.

hour disclosure burden for the FTC-approved COPPA Safe Harbor programs yields an estimated annual labor cost burden of $7,836 (70 hours × $111.94).

b. Annual Audit and Report and Triennial Report for Safe Harbor Programs

FTC staff assumes that compliance officers, at a mean estimated hourly wage of $39.92 in 2025, will prepare annual reports and the triennial report.[686] Applying this hourly labor cost estimate to the hours burden associated with preparing annual audit reports and the annualized burden for the triennial report yields an estimated annual labor cost burden of $14,810 (371 hours × $39.92).

6. Non-Labor/Capital Costs

Because both operators and FTC-approved COPPA Safe Harbor programs will already be equipped with the computer equipment and software necessary to comply with the existing Rule's notice requirements, the amended Rule should not impose any additional capital or other non-labor costs.

IV. Final Regulatory Analysis and Regulatory Flexibility Act Analysis

The Regulatory Flexibility Act (''RFA''), 5 U.S.C. 601 et seq., requires an agency to provide an Initial Regulatory Flexibility Analysis ("IRFA") with a proposed rule and a Final Regulatory Flexibility Analysis ("FRFA") with a final rule unless the Commission certifies that the rule will not have a significant economic impact on a substantial number of small entities. The purpose of a regulatory flexibility analysis is to ensure that an agency considers potential impacts on small entities and examines regulatory alternatives that could achieve the regulatory

[686] *See* BLS Table 1 (compliance officers, $38.55). In order to estimate what the mean hourly wages will be in 2025 ($39.92), staff applies the average growth rate in wages from 2013 through 2023 for compliance officers (1.76%) to the 2023 mean hourly wages ($38.55) for two additional years.

purpose while minimizing burdens on small entities.

In Part II of this document, the Commission adopts many of the amendments the Commission proposed in the 2024 NPRM, adopts some of them with minor modifications, and declines to adopt a small number of them. As discussed in the IRFA in the 2024 NPRM, the Commission believes the amendments it is adopting will not have a significant economic impact on a substantial number of small entities. Among other things, the amendments clarify definitions, increase content requirements for existing notices, increase specificity for existing security requirements, increase clarity for existing retention and deletion requirements, and increase specificity for certain reporting requirements.

Although the amendments will require some entities to implement notices they were not required to provide before, obtain consent they previously were not required to obtain, and implement new retention policies, the Commission believes this will not require significant additional costs for entities covered by the Rule. Instead, the Commission believes some of the amendments, such as an amendment to create an additional exception to the Rule's verifiable parental consent requirement, might even reduce costs for some entities covered by the Rule. Therefore, based on available information, the Commission certifies that the amendments will not have a significant impact on a substantial number of small entities.

While the Commission certifies under the RFA that the amended Rule will not have a significant impact on a substantial number of small entities, and hereby provides notice of that certification to the Small Business Administration (''SBA''), the Commission has determined, nonetheless, that it is appropriate to publish an FRFA to inquire about the impact of the amendments on small entities. Therefore, the Commission has prepared the following analysis:

A. Need for and Objectives of the Amendments

The objectives of the amendments are to update the COPPA Rule to ensure that children's online privacy continues to be protected, as directed by Congress, even as new online technologies emerge and existing online technologies evolve, and to clarify existing obligations for operators under the Rule. The legal basis for the amendments is the Children's Online Privacy Protection Act, 15 U.S.C. 6501 et seq.

B. Significant Issues Raised by Public Comments in Response to the IRFA, the Commission's Assessment and Response, and Any Changes Made as a Result

As discussed in Part II of this document, the Commission received numerous comments that argued that amendments the Commission proposed—including some of the amendments the Commission is now adopting—would be burdensome for businesses. A small number of such comments raised general concerns about the burden that certain proposed amendments would have on small entities. The comments that made assertions about burden did not address the IRFA in particular, or provide empirical evidence about the asserted burdens.

For example, one FTC-approved COPPA Safe Harbor program characterized as "cost and resource prohibitive for small businesses" the Commission's proposed revision to § 312.8 to require operators to establish, implement, and maintain a "comprehensive written security program."[687] As discussed in Part II.F.b, the Commission does not believe that amended § 312.8 will impose significant burdens on small entities. Amended § 312.8 states explicitly, for example, that an operator's size, complexity, and nature and scope of activities, and the sensitivity of the personal information the operator collects from children, are all pertinent factors for determining which information security safeguards are appropriate for the particular

[687] kidSAFE, at 13-14.

operator to establish, implement, and maintain in order to comply with § 312.8.[688] This language will help ensure that amended § 312.8 does not impose undue burdens on small entities.

A trade association asserted that "businesses with smaller staff" might be less able than other businesses to designate employees "to coordinate" an information security program in order to comply with amended § 312.8 "as such coordination would likely be in addition to employees' existing roles."[689] In response to that comment and other comments about § 312.8, the Commission has clarified in Part II.F.b that the employee an operator designates to coordinate its information security program in accord with amended § 312.8(b)(1) may also have other job duties. The Commission believes that clarification addresses the trade association's stated concern.

A different trade association asserted that the proposed amendment to § 312.10 to require operators to provide a written children's personal information retention policy in the online notice required by § 312.4(d) would "burden smaller operators disproportionately in comparison to their larger counterparts that can dedicate time and expenses to crafting, updating, and managing such a public policy."[690] As discussed in Part II.G.b, the Commission has modified proposed § 312.10 to make clearer that amended § 312.10 does not require operators to establish, implement, or maintain a separate, distinct written children's data retention policy as long as they maintain a general written data retention policy that encompasses children's personal information. The Commission believes that modification will help reduce burdens on operators—including "smaller operators"—that have a single, general written data retention

[688] Some commenters asserted that § 312.8 should include consideration of an operator's size as part of the determination of which information security safeguards are appropriate for the operator to establish, implement, and maintain. *See, e.g.*, R Street Institute, at 4.
[689] The Toy Association, at 8.
[690] ANA, at 16.

policy that encompasses children's personal information and would have interpreted amended § 312.10 to require a separate, distinct written children's data retention policy if the Commission had adopted amended § 312.10 as originally proposed in the 2024 NPRM.

In commenting on the proposed amendments to the definition of "website or online service directed to children" in § 312.2 of the Rule, two industry groups asserted that it might be "entirely infeasible" for small entities to comb the Internet for third-party user reviews in order to assess their audience composition.[691] As discussed in Part II.B.5.a.ii, the amended definition of "website or online service directed to children" does not, in fact, require regulated entities to identify and continuously monitor the Internet for such information.

One commenter asserted that the proposed amendment to § 312.4(c)(4) of the Rule to require operators to list in their direct notices the identities or categories of third parties to which they disclose children's personal information would potentially harm small entities by incentivizing regulated entities to work only with large vendors in order to limit the number of third parties to track and update on such lists.[692] As discussed in Part II.C.1.c.ii, the amended Rule will provide operators the flexibility to identify third-party disclosure recipients in their direct notices by name or category. The Commission believes that flexibility addresses the commenter's stated concern.

A commenter asserted that the time and resources needed to implement the human-review component of the face match to verified photo identification verifiable parental consent method the Commission proposed to codify in new § 312.5(b)(2)(vii) would cause small entities to struggle to use the consent method.[693] As discussed in Part II.D.4.b, operators will only bear

[691] Privacy for America, at 6; 4A's, at 2.
[692] *See* Privacy for America, at 10.
[693] *See* American Consumer Institute, at 4.

costs associated with using the particular consent method—which the Commission already approved in November 2015— if they decide to use the method instead of using other verifiable parental consent methods that meet the COPPA Rule's standard of being "reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent."

In response to Question Ten of the "Questions for the Proposed Revisions to the Rule" section of the NPRM, some commenters asserted that amending the Rule to require operators to obtain verifiable parental consent to collect and use persistent identifiers for contextual advertising would negatively affect startup and small entities, in particular.[694] As discussed in Part II.B.4.e, those comments helped inform the Commission's decision not to amend the Rule to require operators to obtain verifiable parental consent to collect and use persistent identifiers for contextual advertising.

A trade association asserted that it would be difficult for its members that are small entities to comply with the Final Rule if the effective date were less than one year after its adoption.[695] Another business coalition similarly asserted that a six-month effective date for the amended rule "may present significant burdens for many small businesses" and recommended "[a]n allowance of up to two years after publication of the final amended Rule" in the Federal Register.[696] As discussed in Part II.I.2.c, the compliance date for most requirements in the Final Rule is one year after publication of the Final Rule in the Federal Register. The Commission believes that compliance date will avoid imposing undue burdens on small entities.

In all, the Commission does not believe it needs to make any changes to its IRFA in

[694] *See, e.g.*, Engine, at 3; 4A's, at 3-4.
[695] *See* The Toy Association, at 9.
[696] *See* Internet Infrastructure Coalition, at 4-5.

response to these comments.

Part II provides a section-by-section analysis that discusses the provisions proposed in the NPRM, the comments received, the Commission's responses to the comments, and any changes made by the Commission as a result.

C. Comments by the Chief Counsel for Advocacy of the SBA, the Commission's Assessment and Response, and Any Changes Made as a Result

The Commission did not receive any comments from the Chief Counsel for Advocacy of the SBA.

D. Description and Estimate of the Number of Small Entities to Which the Rule Will Apply

The COPPA Rule applies to operators of commercial websites or online services directed to children that collect personal information through such websites or online services, and operators of any commercial websites or online services with actual knowledge that they are collecting personal information from children. The Rule also applies to operators of commercial websites or online services that have actual knowledge that they are collecting personal information directly from users of another commercial website or online service directed to children.

Based on the previous estimates and the Commission's compliance monitoring efforts in the areas of children's privacy, FTC staff estimates that approximately 6,140 operators may be subject to the Rule's requirements, with approximately 430 new operators becoming subject to the Rule each year.[697]

Under the Small Business Size Standards issued by the Small Business Administration,

[697] *See* Part III.

"Web Search Publishers and All Other Information Services" qualify as small businesses if the firms have fewer than 1,000 employees, and "Software Publishers" qualify as small businesses if they have $47 million or less in sales. Using 2021 and 2017 Census Statistics of United States Businesses data on the number of firms in the above categories that would qualify as small businesses, FTC staff estimates that approximately 94% to 98% of operators potentially subject to the Rule qualify as small entities.

E. Description of the Projected Reporting, Recordkeeping, and Other Compliance Requirements

The amended Rule will impose reporting, recordkeeping, and other compliance requirements. For example, while not constituting a "collection of information" under the PRA, the amended Rule will require operators to establish, implement, and maintain a written comprehensive security program. The amended Rule will also increase the disclosure requirements for covered operators, and it will increase the disclosure and reporting requirements for FTC-approved COPPA Safe Harbor programs. Specifically, the amendments require operators to update existing disclosures with additional content requirements, namely, to update the direct and online notices with additional information about the operators' information practices. Some operators may have to provide disclosures that the Rule did not previously require. Additionally, the amended Rule requires operators to disclose a data retention policy.

The amended Rule will require each FTC-approved COPPA Safe Harbor program to provide a list of all current subject operators and their certified websites or online services on each of the FTC-approved COPPA Safe Harbor program's websites and online services, and the amended Rule further requires that such list be updated every six months thereafter. The amendments will also require FTC-approved COPPA Safe Harbor programs to include

additional content in their annual reports and submit a new report to the Commission every three years detailing the program's technological capabilities and mechanisms for assessing subject operators' fitness for membership in the program.

The estimated burden imposed by these amendments is discussed in the PRA section of this document. While the Rule's compliance obligations apply equally to all entities subject to the Rule, it is unclear whether the economic burden on small entities will be the same as, or greater than, the burden on other entities. That determination would depend upon a particular entity's compliance costs, some of which may be largely fixed for all entities (e.g., website programming) and others variable (e.g., participation in an FTC-approved COPPA Safe Harbor program), and the entity's income or profit from operation of the website or online service itself (e.g., membership fees) or related sources. As explained in the PRA section, in order to comply with the amended Rule's requirements, website or online service operators will require the professional skills of legal (lawyers or similar professionals) and technical (e.g., computer programmers, software developers, and information security analysts) personnel.

As explained in the PRA section and this FRFA, FTC staff estimates that there are approximately 6,140 websites or online services that qualify as operators under the amended Rule, and that approximately 94% to 98% of such operators qualify as small entities under the SBA's Small Business Size standards.

F. Description of Steps Taken to Minimize Impact of the Rule on Small Entities

As the Commission described in the IRFA, the Commission attempted to tailor each proposed amendment to avoid unduly burdensome requirements for businesses subject to the Rule. Additionally, the Commission built flexibilities into various amendments to reduce burden for all entities subject to the Rule. For example, the amendments the Commission is adopting

permit flexibilities within the information security program, such as to tailor the program to an entity's operations and allow the employee coordinating the program to have other job duties, and within the data retention policy, such as allowing entities to maintain a general written data retention policy that encompasses children's personal information rather than maintaining a separate children's data retention policy. Because the Commission estimates that small entities account for 94% to 98% of entities subject to the Rule, the Commission anticipates that such flexibilities will reduce burden on small entities. In addition, in response to comments, and as discussed in Part II, the Commission has further clarified or modified some of the proposed amendments and has declined to adopt some of the proposed amendments altogether. Those actions should minimize further any economic impact on small entities.

V. Other Matters

Pursuant to the Congressional Review Act (5 U.S.C. 801 et seq.), the Office of Information and Regulatory Affairs designated this rule as not a ''major rule,'' as defined by 5 U.S.C. 804(2).

List of Subjects in 16 CFR Part 312

Communications, Computer technology, Consumer protection, Infants and children, Internet, Privacy, Reporting and recordkeeping requirements, Safety, Science and technology, Trade Practices, Youth.

Accordingly, the Federal Trade Commission revises and republishes 16 CFR part 312 to read as follows:

PART 312—CHILDREN'S ONLINE PRIVACY PROTECTION RULE (COPPA RULE)

Sec.

Authority: 15 U.S.C. 6501 through 6506.

§ 312.1 Scope of regulations in this part.

This part implements the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501, et seq.), which prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

§ 312.2 Definitions.

Child means an individual under the age of 13.

Collects or collection means the gathering of any personal information from a child by any means, including but not limited to:

(1) Requesting, prompting, or encouraging a child to submit personal information online;

(2) Enabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records; or

(3) Passive tracking of a child online.

Commission means the Federal Trade Commission.

Delete means to remove personal information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

Disclose or disclosure means, with respect to personal information:

(1) The release of personal information collected by an operator from a child in identifiable form for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the website or online service; and

(2) Making personal information collected by an operator from a child publicly available in identifiable form by any means, including but not limited to a public posting through the Internet, or through a personal home page or screen posted on a website or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

Federal agency means an agency, as that term is defined in Section 551(1) of title 5, United States Code.

Internet means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of

networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

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, other than for the limited purposes set forth in § 312.5(c), 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.

Obtaining verifiable consent means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child:

(1) Receives notice of the operator's personal information collection, use, and disclosure practices; and

(2) Authorizes any collection, use, and/or disclosure of the personal information.

Online contact information means an email address or any other substantially similar identifier that permits direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, a video chat user identifier, or a mobile telephone number provided the operator uses it only to send text messages to a parent in connection with obtaining parental consent.

Operator means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, or offers products or services for sale through that website or online service, where such website or online service is operated for commercial purposes involving commerce among the several States or with 1 or more foreign nations; in any territory of the United States or in the District of Columbia, or between any such territory and another such territory or any State or foreign nation; or between the District of Columbia and any State, territory, or foreign nation. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45). Personal information is collected or maintained on behalf of an operator when:

(1) It is collected or maintained by an agent or service provider of the operator; or

(2) The operator benefits by allowing another person to collect personal information directly from users of such website or online service.

Parent includes a legal guardian.

Person means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

Personal information means individually identifiable information about an individual collected online, including:

(1) A first and last name;

(2) A home or other physical address including street name and name of a city or town;

(3) Online contact information as defined in this section;

(4) A screen or user name where it functions in the same manner as online contact information, as defined in this section;

(5) A telephone number;

(6) A government-issued identifier, such as a Social Security, state identification card, birth certificate, or passport number;

(7) A persistent identifier that can be used to recognize a user over time and across different websites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier;

(8) A photograph, video, or audio file where such file contains a child's image or voice;

(9) Geolocation information sufficient to identify street name and name of a city or town;

(10) A biometric identifier that can be used for the automated or semi-automated recognition of an individual, such as fingerprints; handprints; retina patterns; iris patterns; genetic data, including a DNA sequence; voiceprints; gait patterns; facial templates; or faceprints; or

(11) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

Release of personal information means the sharing, selling, renting, or transfer of personal information to any third party.

Support for the internal operations of the website or online service means:

(1) Those activities necessary to:

(i) Maintain or analyze the functioning of the website or online service;

(ii) Perform network communications;

(iii) Authenticate users of, or personalize the content on, the website or online service;

(iv) Serve contextual advertising on the website or online service or cap the frequency of advertising;

(v) Protect the security or integrity of the user, website, or online service;

(vi) Ensure legal or regulatory compliance; or

(vii) Fulfill a request of a child as permitted by § 312.5(c)(3) and (4).

(2) Provided, however, that, except as specifically permitted by paragraphs (1)(i)-(vii), the information collected for the activities listed in paragraphs (1)(i)-(vii) of this definition 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.

Third party means any person who is not:

(1) An operator with respect to the collection or maintenance of personal information on the website or online service; or

(2) A person who provides support for the internal operations of the website or online service and who does not use or disclose information protected under this part for any other purpose.

Website or online service directed to children means a commercial website or online service, or portion thereof, that is targeted to children.

(1) In determining whether a website 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 website or online service, as well as whether advertising promoting or appearing on the website 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, including marketing or promotional materials or plans, representations to consumers or to third parties, reviews by users or third parties, and the age of users on similar websites or services.

(2) 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.

(3) A mixed audience website or online service shall not be deemed directed to children with regard to any visitor not identified as under 13.

(4) A website or online service shall not be deemed directed to children solely because it refers or links to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link.

§ 312.3 Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

General requirements. It shall be unlawful for any operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part. Generally, under this part, an operator must:

(a) Provide notice on the website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information (§ 312.4(b));

(b) Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children (§ 312.5);

(c) Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance (§ 312.6);

(d) Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity (§ 312.7); and

(e) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children (§ 312.8).

§ 312.4 Notice.

(a) **General principles of notice**. It shall be the obligation of the operator to provide notice and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children. Such notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials.

(b) **Direct notice to the parent**. An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented.

(c) **Content of the direct notice to the parent** —(1) **Content of the direct notice to the parent for purposes of obtaining consent, including under § 312.5(c)(1)** (Notice to Obtain Parent's Affirmative Consent to the Collection, Use, or Disclosure of a Child's Personal Information). This direct notice shall set forth:

(i) If applicable, that the operator has collected the parent's or child's online contact information from the child, and, if such is the case, the name of the child or the parent, in order to obtain the parent's consent;

(ii) That the parent's consent is required for the collection, use, or disclosure of personal information, and that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide such consent;

(iii) The 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 parent provide consent;

(iv) Where the operator discloses personal information to one or more third parties, the identities or specific categories of such third parties (including the public if making it publicly available) and the purposes for such disclosure, should the parent provide consent, and that the parent can consent to the collection and use of the child's personal information without consenting to the disclosure of such personal information to third parties except to the extent such disclosure is integral to the website or online service;

(v) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section;

(vi) The means by which the parent can provide verifiable consent to the collection, use, and disclosure of the information; and

(vii) If the operator has collected the name or online contact information of the parent or child to provide notice and obtain parental consent, that if the parent does not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the parent's or child's online contact information and the parent's or child's name from its records.

(2) **Content of the direct notice to the parent under § 312.5(c)(2)** (Voluntary Notice to Parent of a Child's Online Activities Not Involving the Collection, Use or Disclosure of Personal Information). Where an operator chooses to notify a parent of a child's participation in a website or online service, and where such site or service does not collect any personal information other than the parent's online contact information, the direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the child in order to provide notice to, and subsequently update the parent about, a child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information;

(ii) That the parent's online contact information will not be used or disclosed for any other purpose;

(iii) That the parent may refuse to permit the child's participation in the website or online service and may require the deletion of the parent's online contact information, and how the parent can do so; and

(iv) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section.

(3) **Content of the direct notice to the parent under § 312.5(c)(4)** (Notice to a Parent of Operator's Intent to Communicate with the Child Multiple Times). This direct notice shall set forth:

(i) That the operator has collected the child's online contact information from the child in order to provide multiple online communications to the child;

(ii) That the operator has collected the parent's online contact information from the child in order to notify the parent that the child has registered to receive multiple online communications from the operator;

(iii) That the online contact information collected from the child will not be used for any other purpose, disclosed, or combined with any other information collected from the child;

(iv) That the parent may refuse to permit further contact with the child and require the deletion of the parent's and child's online contact information, and how the parent can do so;

(v) That if the parent fails to respond to this direct notice, the operator may use the online contact information collected from the child for the purpose stated in the direct notice; and

(vi) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section.

(4) **Content of the direct notice to the parent required under § 312.5(c)(5)** (Notice to a Parent In Order to Protect a Child's Safety). This direct notice shall set forth:

(i) That the operator has collected the name and the online contact information of the child and the parent in order to protect the safety of a child;

(ii) That the information will not be used or disclosed for any purpose unrelated to the child's safety;

(iii) That the parent may refuse to permit the use, and require the deletion, of the information collected, and how the parent can do so;

(iv) That if the parent fails to respond to this direct notice, the operator may use the information for the purpose stated in the direct notice; and

(v) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section.

(d) **Notice on the website or online service**. In addition to the direct notice to the parent, an operator must post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its website or online service, *and*, at each area of the website or online service where personal information is collected from children. The link must be in close proximity to the requests for information in each such area. An operator of a general audience website or online service that has a separate children's area must post a link to a notice of its information practices with regard to children on the home or landing page or screen of the children's area. To be complete, the online notice of the website or online service's information practices must state the following:

(1) The name, address, telephone number, and email address of all operators collecting or maintaining personal information from children through the website or online service. Provided that: The operators of a website or online service may list the name, address, phone number, and email address of one operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or maintaining personal information from children through the website or online service are also listed in the notice;

(2) A description of what information the operator collects from children, including whether the website or online service enables a child to make personal information publicly available; how the operator uses such information; the operator's disclosure practices for such information, including the identities and 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;

(3) 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, or for any other purpose (except as specifically permitted to provide support for the internal operations of the website or online service);

(4) 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; and

(5) If applicable, that the parent can review or have deleted the child's personal information, and refuse to permit further collection or use of the child's information, and state the procedures for doing so.

§ 312.5 Parental consent.

(a) **General requirements**. (1) An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented.

(2) 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 website or online service. An operator required to give the parent this option must obtain separate verifiable parental consent to such disclosure.

(b) **Methods for verifiable parental consent**.

(1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.

(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;

(vi) Verifying a parent's identity using knowledge-based authentication provided:

(A) the verification process uses dynamic, multiple-choice questions, where there are a reasonable number of questions with an adequate number of possible answers such that the probability of correctly guessing the answers is low; and

(B) the questions are of sufficient difficulty that a child age 12 or younger in the parent's household could not reasonably ascertain the answers;

(vii) Having a parent submit a government-issued photographic identification that is verified to be authentic and is compared against an image of the parent's face taken with a phone camera or webcam using facial recognition technology and confirmed by personnel trained to confirm that the photos match; provided that the parent's identification and images are promptly deleted by the operator from its records after the match is confirmed; or

(viii) Provided that, an operator that does not "disclose" (as defined by § 312.2) children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email.

(ix) Provided that, an operator that does not "disclose" (as defined by § 312.2) children's personal information, may use a text message coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory text message to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier text message.

(3) Safe harbor approval of parental consent methods. A safe harbor program approved by the Commission under § 312.11 may approve its member operators' use of a parental consent method not currently enumerated in paragraph (b)(2) of this section where the safe harbor

program determines that such parental consent method meets the requirements of paragraph (b)(1) of this section.

(c) **Exceptions to prior parental consent**. Verifiable parental consent is required prior to any collection, use, or disclosure of personal information from a child except as set forth in this paragraph:

(1) Where the sole purpose of collecting the name or online contact information of the parent or child is to provide notice and obtain parental consent under § 312.4(c)(1). If the operator has not obtained parental consent after a reasonable time from the date of the information collection, the operator must delete such information from its records;

(2) Where the purpose of collecting a parent's online contact information is to provide voluntary notice to, and subsequently update the parent about, the child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information. In such cases, the parent's online contact information may not be used or disclosed for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(2);

(3) Where the sole purpose of collecting online contact information from a child is to respond directly on a one-time basis to a specific request from the child, and where such information is not used to re-contact the child or for any other purpose, is not disclosed, and is deleted by the operator from its records promptly after responding to the child's request;

(4) Where the purpose of collecting a child's and a parent's online contact information is to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from

the child. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(3). An operator will not be deemed to have made reasonable efforts to ensure that a parent receives notice where the notice to the parent was unable to be delivered;

(5) Where the purpose of collecting a child's and a parent's name and online contact information, is to protect the safety of a child, and where such information is not used or disclosed for any purpose unrelated to the child's safety. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to provide a parent with notice as described in § 312.4(c)(4);

(6) Where the purpose of collecting a child's name and online contact information is to:

(i) Protect the security or integrity of the website or online service;

(ii) Take precautions against liability;

(iii) Respond to judicial process; or

(iv) To the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety; and where such information is not used for any other purpose;

(7) Where an operator collects a persistent identifier and no other personal information and such identifier is used for the sole purpose of providing support for the internal operations of the website or online service. In such case, the operator shall provide notice under § 312.4(d)(3);

(8) Where an operator covered under paragraph (2) of the definition of website or online service directed to children in § 312.2 collects a persistent identifier and no other personal information from a user who affirmatively interacts with the operator and whose previous

registration with that operator indicates that such user is not a child. In such case, there also shall be no obligation to provide notice under § 312.4; or

(9) Where an operator collects an audio file containing a child's voice, and no other personal information, for use in responding to a child's specific request and where the operator does not use such information for any other purpose, does not disclose it, and deletes it immediately after responding to the child's request. In such case, there also shall be no obligation to provide a direct notice, but notice shall be required under § 312.4(d).

§ 312.6 Right of parent to review personal information provided by a child.

(a) Upon request of a parent whose child has provided personal information to a website or online service, the operator of that website or online service is required to provide to that parent the following:

(1) A description of the specific types or categories of personal information collected from children by the operator, such as name, address, telephone number, email address, hobbies, and extracurricular activities;

(2) The opportunity at any time to refuse to permit the operator's further use or future online collection of personal information from that child, and to direct the operator to delete the child's personal information; and

(3) Notwithstanding any other provision of law, a means of reviewing any personal information collected from the child. The means employed by the operator to carry out this provision must:

(i) Ensure that the requestor is a parent of that child, taking into account available technology; and

(ii) Not be unduly burdensome to the parent.

(b) Neither an operator nor the operator's agent shall be held liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under this section.

(c) Subject to the limitations set forth in § 312.7, an operator may terminate any service provided to a child whose parent has refused, under paragraph (a)(2) of this section, to permit the operator's further use or collection of personal information from his or her child or has directed the operator to delete the child's personal information.

§ 312.7 Prohibition against conditioning a child's participation on collection of personal information.

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.

§ 312.8 Confidentiality, security, and integrity of personal information collected from children.

(a) The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

(b) At a minimum, the operator must establish, implement, and maintain a written 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 satisfy this requirement, the operator must:

(1) Designate one or more employees to coordinate the operator's 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 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 information security program or any safeguards in place to protect personal information collected from children.

(c) Before allowing other operators, service providers, or third parties to collect or maintain personal information from children on the operator's behalf, or before releasing children's personal information to such entities, the operator must take reasonable steps to determine that such entities are capable of maintaining the confidentiality, security, and integrity of the information and must obtain written assurances that such entities will employ reasonable measures to maintain the confidentiality, security, and integrity of the information.

§ 312.9 Enforcement.

Subject to sections 6503 and 6505 of the Children's Online Privacy Protection Act of 1998, a violation of a regulation prescribed under section 6502 (a) of this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

§ 312.10 Data retention and deletion requirements.

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. When such information is no longer reasonably necessary for the purposes 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 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. The operator must provide its written data retention policy addressing personal information collected from children in the notice on the website or online service provided in accordance with § 312.4(d).

§ 312.11 Safe harbor programs.

(a) **In general**. Industry groups or other persons may apply to the Commission for approval of self-regulatory program guidelines ("safe harbor programs"). The application 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 application. The Commission shall issue a written determination within 180 days of the filing of the application.

(b) **Criteria for approval of self-regulatory program guidelines**. Proposed safe harbor programs must demonstrate that they meet the following performance standards:

(1) Program requirements that ensure operators subject to the self-regulatory program guidelines ("subject operators") provide substantially the same or greater protections for children as those contained in §§ 312.2 through 312.8, and 312.10.

(2) 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. The assessment mechanism required under this paragraph can be provided by an independent enforcement program, such as a seal program.

(3) Disciplinary actions for subject operators' non-compliance with self- regulatory program guidelines. This performance standard may be satisfied by:

(i) Mandatory, public reporting of any action taken against subject operators by the industry group issuing the self-regulatory guidelines;

(ii) Consumer redress;

(iii) Voluntary payments to the United States Treasury in connection with an industry-directed program for violators of the self-regulatory guidelines;

(iv) Referral to the Commission of operators who engage in a pattern or practice of violating the self-regulatory guidelines; or

(v) Any other equally effective action.

(c) **Request for Commission approval of self-regulatory program guidelines**. A proposed safe harbor program's request for approval shall be accompanied by the following:

(1) A detailed explanation of the applicant's business model, and the technological capabilities and mechanisms that will be used for initial and continuing assessment of subject operators' fitness for membership in the safe harbor program;

(2) A copy of the full text of the guidelines for which approval is sought and any accompanying commentary;

(3) A comparison of each provision of §§ 312.2 through 312.8, and 312.10 with the corresponding provisions of the guidelines; and

(4) A statement explaining:

(i) How the self-regulatory program guidelines, including the applicable assessment mechanisms, meet the requirements of this part; and

(ii) How the assessment mechanisms and compliance consequences required under paragraphs (b)(2) and (b)(3) provide effective enforcement of the requirements of this part.

(d) **Reporting and recordkeeping requirements**. Approved safe harbor programs shall:

(1) By [INSERT DATE SIX MONTHS AFTER DATE OF PUBLICATION 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);

(2) Promptly respond to Commission requests for additional information;

(3) Maintain for a period not less than three years, and upon request make available to the Commission for inspection and copying:

(i) Consumer complaints alleging violations of the guidelines by subject operators;

(ii) Records of disciplinary actions taken against subject operators; and

(iii) Results of the independent assessments of subject operators' compliance required under paragraph (b)(2) of this section; and

(4) No later than [INSERT DATE 90 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], publicly post on each of the approved safe harbor program's websites and online services a list of all current subject operators and, for each such operator, list each certified website or online service. Approved safe harbor programs shall update this list every six months thereafter to reflect any changes to the approved safe harbor programs' subject operators or their applicable websites and online services.

(e) **Post-approval modifications to self-regulatory program guidelines**. Approved safe harbor programs must submit proposed changes to their guidelines for review and approval by the Commission in the manner required for initial approval of guidelines under paragraph (c)(2) of this section. The statement required under paragraph (c)(4) of this section must describe how the proposed changes affect existing provisions of the guidelines.

(f) **Review of self-regulatory program guidelines.** No later than [INSERT DATE 3 YEARS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], and every three years thereafter 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.

(g) **Revocation of approval of self-regulatory program guidelines**. 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. Safe harbor programs shall, by [6 MONTHS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], 2025, submit proposed modifications to their guidelines.

(h) **Operators' participation in a safe harbor program**. An operator will be deemed to be in compliance with the requirements of §§ 312.2 through 312.8, and 312.10 if that operator complies with Commission-approved safe harbor program guidelines. In considering whether to initiate an investigation or bring an enforcement action against a subject operator for violations of this part, the Commission will take into account the history of the subject operator's participation in the safe harbor program, whether the subject operator has taken action to remedy such non-compliance, and whether the operator's non-compliance resulted in any one of the disciplinary actions set forth in paragraph (b)(3) of this section.

§ 312.12 Voluntary Commission Approval Processes.

(a) Parental consent methods. An interested party may file a written request for Commission approval of parental consent methods not currently enumerated in § 312.5(b). To be considered for approval, a party must provide a detailed description of the proposed parental consent methods, together with an analysis of how the methods meet § 312.5(b)(1). 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; and

(b) Support for the internal operations of the website or online service. 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.

§ 312.13 Severability.

The provisions of this part are separate and severable from one another. If any provision is stayed or determined to be invalid, it is the Commission's intention that the remaining provisions shall continue in effect.

* * * * *

By direction of the Commission.

April J. Tabor,

Secretary.