FEDERAL TRADE COMMISSION

16 CFR Part 312

RIN 3084–AB20

Children's Online Privacy Protection Rule

AGENCY: Federal Trade Commission.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Commission proposes to amend the Children's Online Privacy Protection Rule, consistent with the requirements of the Children's Online Privacy Protection Act. The proposed modifications are intended to respond to changes in technology and online practices, and where appropriate, to clarify and streamline the Rule. The proposed modifications, which are based on the FTC's review of public comments and its enforcement experience, are intended to clarify the scope of the Rule and/or strengthen its protection of personal information collected from children.

DATES: Comments must be received by March 11, 2024.

ADDRESSES: Interested parties may file a comment online or on paper by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Write ''COPPA Rule Review, Project No. P195404'' on your comment and file your comment online at *https://www.regulations.gov* by following the instructions on the web-based form. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC–5610 (Annex E), Washington, DC 20580.

FOR FURTHER INFORMATION CONTACT: Manmeet Dhindsa (202–326–2877) or James Trilling (202–326–3497), Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission.

SUPPLEMENTARY INFORMATION:

I. Background

Congress enacted the Children's Online Privacy Protection Act (''COPPA'' or ''COPPA statute''), 15 U.S.C. 6501 *et seq.,* in 1998. The COPPA statute directed the Federal Trade Commission (''Commission'' or ''FTC'') to promulgate regulations implementing COPPA's requirements. On November 3, 1999, the Commission issued its Children's Online Privacy Protection Rule, 16 CFR part 312 (''COPPA Rule'' or ''Rule''), which became effective on April 21, 2000.[1] Section 6506 of the COPPA statute and § 312.11 of the initial Rule required that the Commission initiate a review no later than five years after the initial Rule's effective date to evaluate the Rule's implementation. The Commission commenced this mandatory review on April 21, 2005.[2] After receiving and considering extensive public comment, the Commission determined in March 2006 to retain the COPPA Rule without change.[3] In 2010, the Commission once again undertook a review of the COPPA Rule to determine whether the Rule was keeping pace with changing technology. After notice and comment, the Commission issued final amendments to the Rule, which became effective on July 1, 2013 (''2013 Amendments'').[4]

The COPPA Rule imposes certain requirements on operators of websites [5] or online services directed to children under 13 years of age, and on operators of websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age (collectively, ''operators''). The Rule requires that operators provide notice to parents and obtain verifiable parental consent before collecting, using, or disclosing personal information from children under 13 years of age.[6] Additionally, the Rule requires that operators must provide parents the opportunity to review the types or categories of personal information collected from their child, the opportunity to delete the collected information, and the opportunity to prevent further use or future collection of personal information from their child.[7] The Rule also requires operators to keep personal information they collect from children secure, including by imposing retention and deletion requirements, and prohibits them from conditioning children's participation in activities on the collection of more personal information than is reasonably necessary to participate in such activities.[8] The Rule contains a ''safe harbor'' provision enabling industry groups or others to submit to the Commission for approval self-regulatory guidelines that would implement the Rule's protections.[9]

The 2013 Amendments [10] revised the COPPA Rule to address changes in the way children use and access the internet, including through the increased use of mobile devices and social networking. In particular, the 2013 Amendments:

- Modified the definition of ''operator'' to make clear that the Rule covers an operator of a child-directed website or online service that integrates outside services—such as plug-ins or advertising networks—that collect personal information from the website's or online service's visitors, and expanded the definition of ''website or online service directed to children'' to clarify that those outside services are subject to the Rule where they have actual knowledge that they are collecting personal information directly from users of a child-directed website or online service;
- Permitted a subset of child-directed websites or online services that do not target children as their primary audience to differentiate among users, requiring them to comply with the Rule's obligations only as to users who identify as under the age of 13;
- Expanded the definition of ''personal information'' to include geolocation information; photos, videos and audio files containing a child's image or voice; and persistent identifiers that can be used to recognize a user over time and across different websites or online services;
- Streamlined the direct notice requirements to ensure that key information is presented to parents in a succinct ''just-in-time'' notice;
- Expanded the non-exhaustive list of acceptable methods for obtaining prior verifiable parental consent;
- Created three new exceptions to the Rule's notice and consent requirements, including for the use of persistent identifiers for the support for the internal operations of a website or online service;

[1] Children's Online Privacy Protection Rule, Statement of Basis and Purpose, 64 FR 59888 (Nov. 3, 1999), available at *https://www.federalregister.gov/documents/1999/11/03/99-27740/childrens-online-privacy-protection-rule.*

[2] Children's Online Privacy Protection Rule, Request for Public Comment, 70 FR 21107 (Apr. 22, 2005), available at *https://www.federalregister.gov/documents/2005/04/22/05-8160/childrens-online-privacy-protection-rule-request-for-comments.*

[3] Children's Online Privacy Protection Rule, Retention of Rule Without Modification, 71 FR 13247 (Mar. 15, 2006), available at *https://www.federalregister.gov/documents/2006/03/15/06-2356/childrens-online-privacy-protection-rule.*

[4] *See* Children's Online Privacy Protection Rule, Statement of Basis and Purpose, 78 FR 3972 (Jan. 17, 2013), available at *https://www.federalregister.gov/documents/2013/01/17/2012-31341/childrens-online-privacy-protection-rule.*

[5] *See* Part IV for further discussion of the Commission's proposal to change the term ''Web site'' to ''Web site'' throughout the Rule. This Notice of Proposed Rulemaking incorporates this proposed change in all instances in which the term ''Web site'' is used.

[6] 16 CFR 312.3, 312.4, and 312.5.

[7] 16 CFR 312.3 and 312.6.

[8] 16 CFR 312.3, 312.7, 312.8, and 312.10.

[9] 16 CFR 312.11.

[10] 78 FR 3972.

• Strengthened data security protections by requiring operators to take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of such information, and required reasonable data retention and deletion procedures; and

• Strengthened the Commission's oversight of self-regulatory safe harbor programs.[11]

On July 25, 2019, the FTC announced in the **Federal Register** that it was again undertaking a review of the COPPA Rule, noting that questions had arisen about the Rule's application to the educational technology (''ed tech'') sector, voice-enabled connected devices, and general audience platforms that host third-party child-directed content (''2019 Rule Review Initiation'').[12] The Commission sought public comment on these and other issues in its 2019 Rule Review Initiation. In addition to its standard regulatory review questions to determine whether the Commission should retain, eliminate, or modify the COPPA Rule, the Commission asked whether the 2013 Amendments have resulted in stronger protections for children and whether the revisions have had any negative consequences. The Commission also posed specific questions about the Rule's provisions, including the Rule's definitions, notice and consent requirements, access and deletion rights, security requirements, and safe harbor provisions.

During the comment period, the Commission held a public workshop on October 7, 2019, to discuss in detail several of the areas where it sought public comment (''COPPA Workshop'').[13] Specific discussion included such topics as application of the COPPA Rule to the ed tech sector, how the development of new technologies and business models have affected children's privacy, and whether the 2013 Amendments have worked as intended.

In response to the 2019 Rule Review Initiation, the Commission received more than 175,000 comments from various stakeholders, including industry representatives, video content creators, consumer advocacy groups, academics, technologists, FTC-approved COPPA Safe Harbor programs, members of Congress, and individual members of the public. While many of these comments expressed overall support for COPPA,[14] the comments identified a number of areas where the Commission could provide additional clarification or guidance about the COPPA Rule's requirements. The comments also proposed a number of potential changes to the Rule.

Following consideration of the submitted public comments, viewpoints expressed during the COPPA Workshop, and the Commission's experience enforcing the Rule, the Commission proposes modifying most provisions of the Rule. Part II of this notice of proposed rulemaking (''NPRM'') discusses commenters' calls to expand the COPPA Rule's coverage by amending the definition of ''website or online service directed to children'' or by changing the Rule's actual knowledge standard. Part III of this NPRM discusses commenters' viewpoints on whether the Commission should permit general audience platforms that allow third parties to upload content to the platform to rebut the presumption that all users of uploaded child-directed content are children. Part IV addresses the Commission's proposed modifications to the Rule. Parts V–X provide information about requests for comment, the Paperwork Reduction Act, the Regulatory Flexibility Act, communications by outside parties to the Commissioners or their advisors, questions for the proposed revisions to the Rule, a list of subjects in the Rule, and the amended text of the Rule.

II. Comments on Expanding the COPPA Rule's Coverage

As part of its 2019 Rule Review Initiation, the Commission requested comment on questions regarding whether the Commission should revise the definition of ''website or online service directed to children.'' In response, the Commission received various comments regarding expanding the COPPA Rule's coverage by either amending the definition of ''website or online service directed to children'' or by changing the Rule's actual knowledge standard. This Part includes discussion of comments advocating for and against such expansions.

A. Amending the Definition of ''Website or Online Service Directed to Children''

In its 2019 Rule Review Initiation, the Commission asked for comment on various aspects of the Rule's definition of ''website or online service directed to children.'' Among other questions, the Commission asked whether it should amend the definition to address websites and online services that do not include traditionally child-oriented activities but still have large numbers of child users.[15]

Some commenters argued that the definition of ''website or online service directed to children'' should be modified to include sites and services with large numbers of children, those with a certain percentage of child users, or those that include child-attractive

[11] *Id.*

[12] *See* Children's Online Privacy Protection Rule, Request for Public Comment, 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.*

[13] *See The Future of the COPPA Rule: An FTC Workshop* (Oct. 7, 2019), available at *https://www.ftc.gov/news-events/events/2019/10/future-coppa-rule-ftc-workshop;* 84 FR 35842.

[14] *See, e.g.,* Joint Comment of the Attorneys General of New Mexico, Connecticut, Delaware, the District of Columbia, Idaho, Illinois, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Nebraska, Nevada, New York, North Carolina, Oregon, Pennsylvania, Tennessee, Vermont, Virginia, and Washington (''Joint Attorneys General''), at 2 (''As more and more of our lives are lived online, and as digital tools make their way into our schools and into our lives at ever-earlier ages, rules like the COPPA Rule must continue not only to exist, but grow and adapt to ever-changing regulatory landscapes''); SuperAwesome Inc. (''SuperAwesome''), at 8 (''As a result of the rapid evolution of the [I]nternet economy and in particular services that rely on user data, the need for the COPPA Rule has never been greater''); Privacy Vaults Online, Inc. (''PRIVO''), at 2 (''In PRIVO's experience, both children and operators benefit when COPPA-compliant processes are in place to permit operators to offer relevant content to children and permit children to engage with that content in an appropriate and permissioned manner''); The LEGO Group (''Lego''), at 3 (''COPPA has played and continues to play an important role in raising awareness of the importance of protecting children's privacy online. COPPA has been effective because of its future-proof language, which has allowed it to protect against real harms today, that were not clear when the Rule was enacted in 1998''); Internet Association, at 1 (''Nearly 20 years after its adoption, COPPA remains an important mechanism for preserving parental choice with respect to the privacy and security of personal information about children under 13''); Consumer Reports, at 5 (''Due to the increase in connected products generally, and children's products specifically, there is only heightened need for the COPPA rules in the coming years''); and Association of National Advertisers (''ANA''), at 3 (''The current COPPA Rule is protective of children's privacy interests and generally workable for businesses. The FTC has given parents the ability to protect children's privacy and entities clear 'rules of the road' regarding how to comply with COPPA''). *But see* Committee for Justice, at 2 (''In addition to being ineffective at preventing the personal information of children from being collected without parental consent, [COPPA's] approach has the effect of burdening sites targeted towards children''); International Center for Law & Economics (''ICLE''), at 3 (regarding the aggregate costs and benefits of the Rule, ''[t]he benefits are unclear, but the costs—in the form of restricting the ability of family-friendly content creators to monetize their products—are real''); Connected Camps, at 1–3 (stating that COPPA has resulted in a number of unintended consequences based on mistaken assumptions).

[15] Other aspects of this definition are discussed in Part IV.A.5.

content.[16] For example, FTC-approved COPPA Safe Harbor program PRIVO asserted that general audience services with large numbers of children should be required to comply with COPPA, noting that ''[s]ervices not targeted to children that have large numbers of children must be addressed as it can result in online harm to the child due to inherent privacy and safety risks.'' [17] PRIVO further argued that the Commission should define thresholds for the number of child users at which COPPA's protections must be provided.[18] Similarly, Common Sense Media encouraged the Commission to interpret the definition of ''website or online service directed to children'' to include ''sites and services that attract, or are likely to be accessed by, disproportionate numbers of children.'' [19]

However, other commenters opposed expanding the definition of ''website or online service directed to children'' in such ways.[20] For example, The Toy Association opposed the adoption of a numerical or percentage audience threshold as a determinative factor in identifying child-directed websites or online services.[21] Similarly, panelists during the COPPA Workshop noted that ''[a]ttractive to children is very different from targeted to children,'' [22] and that COPPA's statutory language is ''child-directed'' and not ''child-attractive.'' [23] Commenters raised additional concerns with expanding the definition to include sites and services that do not include child-oriented activities but have large numbers of children, including because such a change would be inconsistent with the statute,[24] decrease online offerings for children,[25] be unduly burdensome to operators of non-child-directed websites or online services,[26] and lead to regulatory uncertainty.[27] Some commenters also noted that this amendment would be unnecessary since the definition already includes ''competent and reliable empirical evidence regarding audience composition'' as a factor to consider in determining whether a site or service is directed to children.[28]

During the Rule review that resulted in the 2013 Amendments, the Commission considered amending the definition of ''website or online service directed to children'' to cover sites or services that ''[b]ased on the overall content of the website or online service, [are] likely to attract an audience that includes a disproportionately large percentage of children under age 13 as compared to the percentage of such children in the general population. . . .'' [29] In response, the Commission received numerous comments raising concerns that such a standard was vague, potentially unconstitutional, and unduly expansive, and could lead to widespread age-screening and more intensive age verification across all websites and online services.[30] In ultimately declining to adopt this standard, the Commission stated it did not intend to expand the reach of the Rule to include additional sites and services.

The Commission again declines to modify the Rule in this manner. The definition of ''website or online service directed to children'' includes a number of factors the Commission will consider in determining whether a particular website or online service is child-directed, including consideration of ''competent and reliable empirical evidence regarding audience composition.'' Because the Commission already considers the demographics of a website's or online service's user base in its determination, the Commission does not believe it is necessary to modify the definition.

Similarly, the Commission also previously considered amending the Rule to set forth that websites and online services with a specified percentage of child users would be considered directed to children. As part of the Rule review that led to the 2013 Amendments, the Institute for Public Representation recommended that the Commission amend the Rule so that a website per se should be deemed ''directed to children'' if audience demographics show that 20% or more of its visitors are children under age 13.[31] The Commission determined not to adopt this as a per se legal standard, in part because the Commission noted that the definition of ''website or online service directed to children'' already positions the Commission to consider empirical evidence of the number of child users on a site.

While the Commission continues to believe that there are good reasons not to ground COPPA liability simply on an assessment of the percentage of a site's or service's audience that is under 13, the Commission would like to obtain additional comment on whether it should provide an exemption under which an operator's site or service would not be deemed child-directed if the operator undertakes an analysis of the site's or service's audience composition and determines that no more than a specific percentage of its users are likely to be children under 13. In particular, the Commission seeks comment on (1) whether the Rule should provide an exemption or other incentive to encourage operators to conduct an analysis of their sites' or services' user bases; (2) what the reliable means are by which operators can determine the likely ages of a site's or service's users; (3) whether and how the COPPA Rule should identify such means; (4) what the appropriate percentage of users should be to qualify for this potential exemption; [32] and (5)

[16] *See, e.g.,* Children's Advertising Review Unit (''CARU''), at 6–7; PRIVO, at 7; Common Sense Media, at 12.

[17] PRIVO, at 7.

[18] *Id.*

[19] Common Sense Media, at 12, 15–17.

[20] *See, e.g.,* Computer & Communications Industry Association (''CCIA''), at 6–7; U.S. Chamber of Commerce, at 3–4; ANA, at 6–7; Network Advertising Initiative (''NAI''), at 3–5; ViacomCBS Inc. (''Viacom''), at 5–6; Internet Association, at 9; Entertainment Software Association (''ESA''), at 8–12; TechFreedom, at 18.

[21] The Toy Association, at 9–10 (adding that ''[d]oing so is inconsistent with traditional norms for advertising and risks undermining the intent of the statute by elevating a single factor over others. Such an approach is also entirely inconsistent with how the FTC and advertising self-regulatory bodies handle advertising'').

[22] P. Aftab, Remarks from the *Scope of the COPPA Rule* panel at *The Future of the COPPA Rule: An FTC Workshop* 52 (Oct. 7, 2019), available at *https://www.ftc.gov/news-events/events/2019/10/future-coppa-rule-ftc-workshop.*

[23] *See* D. McGowan, Remarks from the *Scope of the COPPA Rule* panel at *The Future of the COPPA Rule: An FTC Workshop* 48 (Oct. 7, 2019), available at *https://www.ftc.gov/news-events/events/2019/10/future-coppa-rule-ftc-workshop.*

[24] *See, e.g.,* CCIA, at 6; NAI, at 3; ANA, at 6; Viacom, at 5–6; U.S. Chamber of Commerce, at 3–4.

[25] *See, e.g.,* ANA, at 7 (noting that ''[b]roadening the Rule's scope by making it applicable to websites or online services that do not include traditionally child-oriented activities, but that have large numbers of child users, would negatively impact consumers and children because operators would be disincentivized from producing content, products, and online services that, while not directed to them, have the potential to attract child users'').

[26] *See, e.g.,* CCIA, at 7 (noting that ''[a]udience metrics alone are a poor basis for determining COPPA applicability because they can shift over time, may be highly responsive to fads, cannot necessarily be predicted by an operator at the outset of (launching a website or online service, and cannot be reliably calculated'').

[27] *See, e.g.,* ESA, at 8.

[28] *See, e.g.,* CCIA, at 6–7; ANA, at 6–7.

[29] Children's Online Privacy Protection Rule, Supplemental Notice of Proposed Rulemaking; Request for Comment, 77 FR 46643, 46646 (Aug. 6, 2012), available at *https://www.federalregister.gov/documents/2012/08/06/2012-19115/childrens-online-privacy-protection-rule.*

[30] *See* 78 FR 3972 at 3983–3984.

[31] Children's Online Privacy Protection Rule, Proposed Rule; Request for Comment, 76 FR 59804, 59814 (Sept. 27, 2011), available at *https://www.federalregister.gov/documents/2011/09/27/2011-24314/childrens-online-privacy-protection-rule.*

[32] Because this exemption would rely on a single factor (*i.e.,* audience composition) to exempt sites or services from being deemed child-directed, the Commission anticipates that the appropriate

whether such an exemption 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.

B. Changing the COPPA Rule's ''Actual Knowledge'' Standard

In responding to the Commission's request for comment on the definition of ''website or online service directed to children,'' a number of commenters recommended that the Commission revise COPPA's actual knowledge standard by moving to a constructive knowledge standard.[33] Namely, these commenters sought to bring within COPPA's jurisdiction those operators that have reason to know they may be collecting information from a child and those operators that willfully avoid gaining actual knowledge that they are collecting information from a child. Common Sense Media, for example, encouraged the Commission to broaden its view of ''actual knowledge'' to prevent the ''willful disregard that children's personal[ ] information is being collected.'' [34] Other commenters, referencing the California Consumer Privacy Act, similarly recommended that COPPA's actual knowledge standard should cover operators of general audience sites and services that ignore or willfully disregard the age of their users.[35] Children's privacy advocate 5Rights Foundation further recommended that the Commission should consider current and historic audience composition evidence of both the specific service and similar services in determining whether an operator has met the actual knowledge standard.[36]

A number of industry commenters opposed the Commission adopting a constructive knowledge standard. Several of these commenters pointed to the COPPA statute's language [37] and argued that the Commission lacks authority to change the actual knowledge standard.[38] Others asserted that a constructive knowledge standard would result in operators collecting additional data from all users, including children, and might lead to a reduction in available online content because operators may decide to withdraw content intended for teenagers and young adults to avoid the risk of interacting with children.[39] Additionally, the Association of National Advertisers stated that a constructive knowledge standard would conflict with the Commission's long-established position that operators are not obligated to investigate the age of their users [40] and would increase uncertainty about companies' potential COPPA obligations.[41] Similarly, Engine, a non-profit policy organization, noted that moving from the ''bright-line'' standard of actual knowledge to a less clear constructive knowledge standard could disproportionately burden small companies and start-ups.[42]

The Commission declines to change the Rule to bring operators of general audience sites and services under COPPA's jurisdiction based on constructive knowledge. As the Commission noted in 2011, Congress has already rejected a constructive knowledge approach with respect to COPPA. Specifically, the legislative history indicates that Congress originally drafted COPPA to apply to operators that ''knowingly'' collect personal information from children, a standard which would include actual, implied, or constructive knowledge.[43] After consideration of witness testimony, however, Congress modified the knowledge standard in the final legislation to require ''actual knowledge.'' [44] This deliberate decision to reject the more expansive approach makes clear that Congress did not intend for the ''actual knowledge'' standard to be read to include the concept of constructive knowledge. The Commission rejected calls for a move to a lesser knowledge standard for general audience operators while considering the 2013 Amendments,[45] and the Commission again declines to do so.[46]

III. Comments on the Rebuttable Presumption

Operators of websites or online services directed to children that collect personal information from their users must comply with COPPA regardless of whether they have actual knowledge that a particular user is, in fact, a child. Accordingly, as a practical matter, operators of child-directed sites and services must presume that all users are children.[47]

Through the 2013 Amendments, the Commission extended COPPA liability to operators that have actual knowledge

percentage to qualify for this exemption would be very low.

[33] *See, e.g.,* London School of Economics and Political Science, at 9 (noting that the FTC should re-examine its definition of child-directed websites and online services to include '''constructive knowledge' *i.e.,* what an operator ought to know about its users if they have carried their work in due diligence'') (bold typeface omitted); S. Egelman, at 3–4 (asserting that ''actual knowledge'' should include third-party recipients of data from a mobile app that can be identified as child-directed); Color of Change, at 4–5 (advocating that the FTC should move from an actual knowledge standard to a constructive knowledge standard); SuperAwesome, at 18 (recommending the Commission amend the definition of ''website or online service directed to children'' to include situations where an operator has, or should be reasonably expected to have, actual knowledge that it is collecting information from children or from users of a child-directed website or online service).

[34] Common Sense Media, at 12.

[35] 5Rights Foundation, at 3–4; Consumer Reports, at 8–9.

[36] 5Rights Foundation, at 4.

[37] 15 U.S.C. 6502(a)(1) (providing that ''[i]t is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b)'').

[38] *See, e.g.,* ANA, at 4–5; Interactive Advertising Bureau (''IAB''), at 4–5; internet Association, at 19; Software & Information Industry Association (''SIIA''), at 4; The Toy Association, at 3, 8, 10, 16.

[39] *See, e.g.,* Family Online Safety Institute (''FOSI''), at 6 (noting that ''[i]f a constructive knowledge standard were imposed, it is likely that all general audience sites and services would start treating all users as children, or turn off any services that might benefit minors clearly older than 13. This would have serious implications for free speech, or could lead to an increase in age gating, which is ineffective and often results—paradoxically—in increased collection of data from all users, including children''); Digital Content Next, at 1 (stating that ''[w]e believe that expanding the actual knowledge standard might inadvertently harm the privacy of children in two ways. First, if COPPA were expanded to apply in situations where a company has no actual knowledge that the consumer is under 13 years of age or when the company is not providing services directed to children, companies would need to collect significantly more data from children and their parents or guardians to meet the obligations of COPPA including obtaining consent. Second, in order to avoid COPPA compliance, some companies may decide to withdraw content that is intended for teenagers or young adults in order to avoid the risk of interacting with children'').

[40] *See, e.g.,* 64 FR 59888 at 59892 (noting that ''COPPA does not require operators of general audience sites to investigate the ages of their site's visitors . . .'').

[41] *See* ANA, at 5.

[42] Engine, at 5.

[43] *See* 76 FR 59804 at 59806, n. 26 (citing Senate and House bills), noting that ''Under federal case law, the term 'knowingly' encompasses actual, implied, and constructive knowledge.''

[44] *Id.* (citing *internet Privacy Hearing: Hearing on S. 2326 Before the Subcomm. On Commc'ns of the S. Comm. On Commerce, Science, & Transp.,* 105th Cong. 1069 (1998)).

[45] *See* 76 FR 59804 at 59806.

[46] As noted above, various commenters recommended that the Rule's actual knowledge standard cover operators of general audience sites and services that ignore or willfully disregard the age of their users. *See, e.g.,* Common Sense Media, at 12; 5Rights Foundation, at 3–4; Consumer Reports, at 8–9.

The concept of actual knowledge includes willful disregard. *See, e.g., Glob.-Tech Appliances, Inc.* v. *SEB S.A.,* 563 U.S. 754, 766 (2011) (noting that ''[i]t is also said that persons who know enough to blind themselves to direct proof of critical facts in effect have actual knowledge of those facts''). Therefore, the Rule already applies to instances in which an operator of a general audience site or service willfully disregards the fact that a particular user is a child.

[47] *See, e.g.,* 78 FR 3972 at 3984 (''The Commission retains its longstanding position that child-directed sites or services whose primary target audience is children must continue to presume all users are children and to provide COPPA protections accordingly'').

they are collecting personal information directly from the users of another website or online service that is child-directed.[48] Under the Rule, such an operator ''has effectively adopted that child-directed content as its own and that portion of its service may appropriately be deemed to be directed to children.'' [49]

The Commission sought comments in its 2019 Rule Review Initiation on whether it should permit general audience platforms that allow third parties to upload content to the platform to rebut the presumption that all users of uploaded child-directed content are in fact children. In seeking comment on this issue, the Commission stated that absent actual knowledge that the uploaded content is child-directed, the platform operator is not responsible for complying with the Rule. Therefore, the FTC noted that the platform operator may have an incentive to avoid gaining knowledge about the nature of the uploaded content.[50] The Commission asked whether allowing general audience platform operators to rebut this presumption, thereby allowing them to treat users under age 13 differently from older users, would incentivize platform operators to take affirmative steps to identify child-directed content and treat users of that content in accordance with the Rule. The Commission also asked about the types of steps platforms could take to overcome the presumption that all users of child-directed content are children.

Relying on a variety of arguments, many consumer and privacy advocates opposed the notion of modifying the Rule to allow operators of general audience platforms to rebut the presumption that users of child-directed content uploaded to the platform by third parties are children. For example, a coalition of consumer organizations argued against allowing general audience platforms to rebut the presumption, pointing to the fact that families often share devices, accounts, and apps and that, as a result, many children likely access child-directed content while logged into a parent's account. Because of this, they argued that if the FTC modifies the presumption, ''it would lead to widespread mislabeling of children as adults and large numbers of under-protected children.'' [51] Other commenters echoed the concern that because users in a household may share devices that are persistently signed in, operators may incorrectly determine that a user is an adult.[52]

Another commenter, while acknowledging the ''perverse incentive'' operators have to avoid gaining actual knowledge, raised concern about operators' ability to effectively establish which of their users are children.[53] The commenter argued that, until operators are transparent about methods used to determine which users are children and such methods are deemed effective, permitting operators to rebut the presumption may result in children being treated as adults.[54]

One commenter argued that, ''in the vast majority of cases,'' users of child-directed content are, in fact, children.[55] This commenter further stated that allowing operators to rebut the presumption would prioritize allowing companies to engage in targeted advertising over ensuring that general audience platforms comply with COPPA.[56] Another commenter noted that, despite the alleged existence of subcultures of adult viewership of kids' content, the adult viewership of such content is likely very small.[57] The commenter further argued that protecting those adults' right to receive personalized advertising does not outweigh the risk of collecting personal data from children and tracking them online.[58]

A number of State Attorneys General argued that modifying the Rule to allow rebuttal is unlikely to incentivize platforms to identify and police child-directed content.[59] These commenters claimed that, even with the ability to rebut the presumption, platforms would have a greater incentive not to know about the presence of child-directed content because this would allow them to collect data for targeted ads from all users.[60] Additionally, an FTC-approved COPPA Safe Harbor program argued that allowing rebuttal would ''be complex and unfairly benefit large tech companies who may be the only companies with the wherewithal, rich customer data, and back-end infrastructure to meet the criteria for rebuttal.'' [61]

On the other hand, a number of industry commenters supported allowing general audience platforms to rebut the presumption that all users of child-directed content are necessarily children. Google argued that rebuttal ''with the appropriate safeguards, would allow those users to benefit from social engagement with the content and would allow content creators to benefit from increased monetization options, supporting continued investment in such content.'' [62] Without the ability to rebut the presumption, Google argued that platforms must degrade adults' user

[48] *See* 16 CFR 312.2, definition of ''website or online service directed to children,'' paragraph 2.

[49] 78 FR 3972 at 3978.

[50] 84 FR 35842 at 35845–35846. In extending liability to operators of general audience sites and services with actual knowledge, the Commission discussed, but expressly rejected, imposing a ''reason to know'' standard. 78 FR 3972 at 3977–78. Accordingly, the 2013 Amendments do not impose a duty on operators of general audience websites and online services to investigate whether they are collecting personal information from users of child-directed sites or services.

[51] Georgetown University Law Center's Institute for Public Representation submitted a joint comment on behalf of the following nineteen consumer groups: Campaign for a Commercial-Free Childhood; The Center for Digital Democracy; Alana Institute; American Academy of Pediatrics; Badass Teachers Association; Berkeley Media Studies Group; Consumer Action; Consumer Watchdog; Defending the Early Years; Electronic Frontier Foundation; Obligation, Inc.; P.E.A.C.E (Peace Educators Allied for Children Everywhere); Parent Coalition for Student Privacy; Parents Across America; Parents Television Council; Public Citizen; Story of Stuff; TRUCE (Teachers Resisting Unhealthy Childhood Entertainment); and U.S. PIRG (''Joint Consumer Groups''), at iii, 35–36.

[52] *See, e.g.,* Consumer Reports, at 19 (''[B]rowsers and other connected services are increasingly using always-logged-in features in order to make the browsing experience more seamless across devices . . . Although this allows the company to easily sync data across devices, it means that if a child then uses that device to go to YouTube [K]ids or another service it will appear that an adult is logged on and viewing the content''); SuperAwesome, at 28 (''Given the prevalence of shared devices, the only current method to safely detect whether a child or an adult is viewing particular content is by virtue of the type of content. E.g., preschool content is mostly likely viewed by preschoolers. We are particularly concerned about logged-in parents on kids' content, where there is a presumption that the adult is enjoying the kids' content. In our experience, this is rarely the case. In the vast majority of situations it is a child using an adult's device. For this reason, the only safe approach is to default to considering the user a child based on a subjective assessment of the content'') (bold typeface omitted).

[53] 5Rights Foundation, at 4 (also arguing that that the most privacy-protective way of addressing the incentive is to make it more difficult for operators to avoid gaining actual knowledge). *See also* Consumer Reports, at 18–19 (raising concern about the lack of transparency as to how general audience services determine the population of children that use the service).

[54] 5Rights Foundation, at 4.

[55] Consumer Reports, at 19.

[56] *Id.*

[57] SuperAwesome, at 27.

[58] *Id. See also* P. Aftab, at 15 (arguing that the convenience of adults accessing child-directed material should not outweigh children's privacy).

[59] Joint Attorneys General, at 13–14 (adding that they do not support permitting a rebuttable presumption absent robust measures—beyond logged in status or periodic reauthorization—to confirm a user is 13 or older, stating that such measures can include requiring operators to ask during the account creation process whether a child ever uses the account holder's device).

[60] *Id.* At 13.

[61] kidSAFE, at 13 (also suggesting that the Rule's existing mixed audience category could potentially serve the underlying purpose of not treating child-directed content audiences as exclusively under 13).

[62] Google, at 7–8, 11–12 (also arguing that allowing rebuttal does not require a Rule modification because the presumption is not codified in the COPPA statute or Rule).

experience, including by preventing interactivity with other adults. Google also distinguished general audience platforms with third-party content from ''static'' child-directed websites intended for a single audience, noting that such platforms ''have significant adult user bases that engage with traditionally child-directed content.'' [63]

Other commenters made similar arguments. One trade association stated that some general audience platforms ''have significant adult user bases'' and feature child-directed content that may appeal to users of varying ages, such as crafting or science education content.[64] It claimed that the audience presumption harms adult users of child-directed content by denying them the ability ''to find community, learn, and discover new content.'' [65] Another trade association noted that adults might want ''to interact with child-directed content for a variety of reasons, including nostalgia or to find content suitable for their children or students.'' [66]

A majority of the commenters that support modifying the Rule to permit rebuttal also recommended against the Commission proscribing specific means by which a general audience platform could rebut the presumption, calling instead for a flexible, standards-based approach that would allow platforms to employ a variety of measures to overcome the presumption. For example, citing ''advancements in technology and age-screening,'' one trade association recommended allowing rebuttal through reliance on a neutral age gate combined with additional steps to confirm identity, such as re-entry of a password.[67] The commenter also suggested that the Commission allow industry to explore alternative methods such as fingerprint, voiceprint, or device PIN.[68] Other commenters recommended similar flexibility in approach.[69]

Many of the comments supporting rebuttal of the presumption also argued against tying rebuttal to a requirement that the platform investigate and identify child-directed content on the platform. These commenters asserted that such a requirement would change the Rule's actual knowledge standard to a constructive knowledge standard, which would ''contravene [c]ongressional intent'' [70] and impose an unreasonable burden on platforms that would chill investment into the production of child-directed content.[71] One commenter cautioned that requiring the platform operators to identify whether uploaded content is child-directed could raise First Amendment concerns.[72]

After reviewing the submitted comments, the Commission does not propose modifying the Rule to permit general audience platforms to rebut the presumption that all users of child-directed content are children. The Commission finds persuasive the concerns raised in the comments about the practicality of allowing operators of such platforms to rebut this presumption. In particular, the Commission believes that the reality of parents and children sharing devices, along with account holders remaining perpetually logged into their accounts, could make it difficult for an operator to distinguish reliably between those users who are children and those who are not.

The Commission recognizes that allowing platforms to rebut the presumption would permit additional forms of monetization and, in some instances, provide additional functionality and convenience for adults interacting with child-directed content. Such benefits, however, simply do not outweigh the important goal of protecting children's privacy. Moreover, as set forth in the Commission's 2019 Rule Review Initiation, the reason for considering whether to allow platforms to rebut the audience presumption was to create an incentive for them to ''identify and police child-directed content uploaded by others.'' [73] Many commenters supporting the addition of this rebuttal expressed strong opposition to such a duty, thereby undercutting the rationale for modifying the Rule.

Finally, through its recognition of the ''mixed audience'' category of websites and online services, the Commission essentially allows operators to rebut the presumption as to the users of a subset of child-directed sites and services that do not target children as their primary audience. For example, where third-party content on a platform is child-directed under the Rule's multi-factor test but the platform does not target children as its primary audience, the operator can request age information and provide COPPA protections only to those users who are under 13. The Commission believes the mixed audience category affords operators an appropriate degree of flexibility.[74]

IV. Proposed Modifications to the Rule

As discussed in Part I, comments reflect overall support for COPPA and a recognition that it is an important and helpful tool for protecting children's online privacy. Additionally, many comments indicate support for the 2013 Amendments.[75]

[63] *Id.* At 8.

[64] SIIA, at 5.

[65] *Id.*

[66] CCIA, at 13.

[67] internet Association, at 18–19.

[68] *Id.* At 19.

[69] *See* Centre for Information Policy Leadership (''CIPL''), at 7 (supporting rebuttal where platforms take reasonable steps such as a neutral age gate plus additional verification, adding that the Commission should permit companies to adopt their own approach as long as they meet certain standards set by FTC); CCIA, at 14 (recommending the FTC adopt an ''adaptable standards-based approach'' for permitting general audience services to treat adult users interacting with child-directed content as adults, including the use of neutral age screening in conjunction with periodic password reauthorization and ''verification methods that may be appropriate in additional contexts, such as submitting a voiceprint or device PIN''); Google, at 10–11 (recommending the FTC adopt a ''reasonably calculated'' standard similar to the parental consent standard that provides reasonable assurance that the person engaging with the content is an adult, and further suggesting use of a neutral age gate in combination with such mechanisms as password re-authentication, fingerprint, or device PINs); SIIA, at 5 (supporting a ''standards-based approach to rebut presumption relying on neutral age gates plus additional steps like password authorization or alternative verification methods''); U.S. Chamber of Commerce, at 7 (supporting an adaptable standards-based approach rather than prescriptive measures); Yoti, at 16 (supporting the various mechanisms suggested in the Commission's 2019 Rule Review Initiation, but adding that because some may not work in certain circumstances, they should be options as opposed to a mandatory list).

[70] CCIA, at 14.

[71] *See* U.S. Chamber of Commerce, at 7; ANA, at 5–6; Google, at 11.

[72] Center for Democracy & Technology (''CDT''), at 9 (further adding that the Commission should not consider costs and benefits unrelated to privacy (*e.g.,* exposure to age-inappropriate content) as such concerns fall outside COPPA's statutory focus). *But see* SuperAwesome, at 29 (recommending the Commission consider costs and benefits unrelated to privacy, noting that allowing a rebuttal ''will significantly increase the risk of exposing children to inappropriate content, including inappropriate advertising, and potentially dangerous user-generated content'').

[73] 84 FR 35842 at 35846.

[74] While it is possible that the sharing of devices between parents and children can lead to complexities in determining the ''mixed audience'' nature of a website or online service, the Commission believes on balance that there is value in continuing to allow for a mixed audience designation.

[75] *See, e.g.,* SuperAwesome; PRIVO; ESA; Electronic Privacy Information Center (''EPIC''); and Joint Consumer Groups. *But see, e.g.,* Skyship Entertainment; J. Johnston (J House Vlogs); H. and S. Jho (Sockeye Media LLC); and ICLE. These commenters, many of whom are content creators on YouTube, opposed the Rule changes and/or the FTC's 2019 enforcement action against Google LLC and its subsidiary YouTube, LLC (''YouTube Case''), *Federal Trade Commission & People of the State of New York* v. *Google LLC & YouTube, LLC,* Case No. 1:19–cv–2642 (D.D.C. 2019), *available at https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3083-google-llc-youtube-llc.* These commenters asserted that the 2013 Amendments and the YouTube Case have affected the availability of children's content on YouTube due to creators' inability to monetize through personalized advertisements. Additional commenters criticized the 2013 Amendments for other reasons, such as

Continued

Despite this overall support, the Commission believes it is appropriate to modify a number of the Rule's provisions in light of the record developed through the 2019 Rule Review Initiation—including the COPPA Workshop and the large number of public comments received—as well as the FTC's two decades of experience enforcing the Rule. The Commission intends these modifications to update certain aspects of the Rule, taking into account technological and other relevant developments, and to provide additional clarity to operators on the Rule's existing requirements. Specifically, the Commission proposes modifying most provisions of the Rule, namely the following areas: Definitions; Notice; Parental Consent; Parental Right to Review; Confidentiality, Security, and Integrity of Children's Personal Information; Data Retention and Deletion; and Safe Harbor Programs. In addition, the Commission proposes minor modifications to the sections on Scope of Regulations and Voluntary Commission Approval Processes to address technical corrections.

Additionally, the Commission proposes some revisions to the Rule to address spelling, grammatical, and punctuation issues. For example, as noted above, the Commission proposes to modify § 312.1 regarding the scope of regulations, specifically to change the location of commas. Similarly, the Commission proposes amending the Rule to change the term ''Web site'' to ''website'' throughout the Rule, including in various definitions that use this term. This construction aligns with the COPPA statute's use of the term, as well as how that term is currently used in today's marketplace. This NPRM incorporates this proposed change in all instances in which the term ''Web site'' is used. The Commission does not intend for these proposed modifications to alter existing obligations or create new obligations under the Rule.

A. Definitions (16 CFR 312.2)

The Commission proposes to modify a number of the Rule's definitions in order to update the Rule's coverage and functionality and, in certain areas, to provide greater clarity regarding the Rule's intended application. The Commission proposes modifications to the definitions of ''online contact information'' and ''personal information.'' The Commission also proposes modifications to the definition of ''website or online service directed to children,'' including by adding a stand-alone definition for ''mixed audience website or online service.'' Additionally, the Commission proposes adding definitions for ''school'' and ''school-authorized education purpose.'' These two new definitions relate to the Rule's proposed new parental consent exception—a codification of longstanding Commission guidance by which operators rely on school authorization to collect personal information in limited circumstances rather than on parental consent. Finally, the Commission proposes modifications to the second paragraph of the definition of ''support for the internal operations of the website or online service.''

1. Online Contact Information

Section 312.2 of the Rule defines ''online contact information'' as ''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, or a video chat user identifier.'' Online contact information is considered ''personal information'' under the Rule. Under certain parental consent exceptions, the Rule permits operators to collect online contact information from a child for certain purposes, such as initiating the process of obtaining verifiable parental consent, without first obtaining verifiable parental consent.

To improve the Rule's functionality, the Commission proposes amending this definition by adding ''an identifier such as a mobile telephone number provided the operator uses it only to send a text message'' to the non-exhaustive list of identifiers that constitute ''online contact information.'' As discussed later in this Part, this modification would allow operators to collect and use a parent's or child's mobile phone number in certain circumstances, including in connection with obtaining parental consent through a text message.

Although the Commission did not raise the issue of adding mobile telephone numbers to the online contact information definition in its 2019 Rule Review Initiation, some commenters supported such a modification in discussing the Rule's parental consent requirement.[76] One commenter noted that parents increasingly rely on telephone and cloud-based text messaging services,[77] and another similarly noted that permitting parents to utilize text messages to provide consent would be more in sync with current technology and parental expectations.[78] Commenters also stated that mobile communication mechanisms are more likely to result in operators reaching parents for the desired purpose of providing notice and obtaining consent, and that sending a text message may be one of the most direct and easily verifiable methods of contacting a parent.[79] Further, one commenter posited that the chance of a child submitting his or her own mobile number in order to circumvent a valid consent mechanism is no greater than, for instance, a child submitting his or her own email address.[80]

The Commission agrees that permitting parents to provide consent via text message would offer them significant convenience and utility. The Commission also recognizes that consumers are likely accustomed to using mobile telephone numbers for account creation or log-in purposes. For these reasons, the Commission is persuaded that operators should be able to collect parents' mobile telephone numbers as a method to obtain consent from the parent. Therefore, the Commission proposes adding mobile telephone numbers to the definition of ''online contact information.''

Modifying the definition in this way, however, will also enable operators to collect and use a child's mobile telephone number to communicate with the child, including—under various parental consent exceptions—prior to the operator obtaining parental consent.[81] The Commission does not seek to allow operators to use children's mobile telephone numbers to call them prior to the operator obtaining parental consent. Therefore, the Commission proposes including the qualifier ''provided the operator uses it only to send a text message'' to ensure that operators cannot call the child using the mobile telephone number, unless and until the operator seeks and obtains a parent's verifiable parental consent to do so.[82]

purported negative consequences to industry or beliefs that the 2013 Amendments strayed from the purpose of the COPPA statute. *See, e.g.,* Committee for Justice; TechFreedom; and Competitive Enterprise Institute.

[76] *See, e.g.,* kidSAFE, at 3–4. More generally, several other commenters recommended modifying the Rule to allow the use of text messaging in connection with obtaining parental consent. *See* The Toy Association, at 4; ESA, at 24–26; ANA, at 12; Entertainment Software Rating Board (''ESRB''), at 8.

[77] kidSAFE, at 4.

[78] ESA, at 24–25.

[79] kidSAFE, at 3–4; ANA, at 12.

[80] kidSAFE, at 4.

[81] 16 CFR 312.5(c)(1), (3), (4), (5), and (6).

[82] Because various parental consent exceptions allow operators to collect a child's ''online contact information'' without first obtaining verifiable parental consent, the Commission proposes limiting operators from using such information to call a child. However, this proposal does not prevent an

This proposed modification is a departure from the position the Commission previously took when it declined to include mobile telephone numbers within the definition of ''online contact information.'' In discussing the 2013 Amendments, the Commission stated that the COPPA statute did not contemplate adding mobile telephone numbers as a form of online contact information, and therefore it determined not to include mobile telephone numbers within the definition.[83] However, the Commission also stated at that time that the list of identifiers constituting online contact information was non-exhaustive and would encompass other substantially similar identifiers that permit direct contact with a person online.[84] As part of the 2013 Amendments, the Commission revised the definition to include examples of such identifiers, and the Commission now believes that adding mobile telephone numbers to this list is appropriate.

Specifically, consumers today widely use over-the-top messaging platforms, which are platforms that utilize the internet instead of a carrier's mobile network to exchange messages. These platforms include Wi-Fi messaging applications, voice over internet protocol applications that have messaging features, and other messaging applications. Because a consumer's mobile telephone number is often used as the unique identifier through which a consumer can exchange messages through these over-the- top platforms, mobile telephone numbers permit direct contact with a person online, thereby meeting the statutory requirements for this definition.[85]

When the Commission enacted the 2013 Amendments, the use of over-the-top messaging platforms was more nascent and growing in adoption. Today, the prevalent and widespread adoption of such messaging platforms allows consumers to use these platforms as their primary form of text messaging. Therefore, the Commission finds it appropriate to propose amending the definition of ''online contact information'' to include ''an identifier such as a mobile telephone number provided the operator uses it only to send a text message.'' The Commission welcomes comment on this proposed modification. In particular, the Commission is interested in understanding whether allowing operators to contact parents through a text message to obtain verifiable parental consent presents security risks to the recipient of the text message, especially if the parent would need to click on a link provided in the text message.

2. Personal Information

The COPPA statute defines ''personal information'' as individually identifiable information about an individual collected online, including, for example, a first and last name, an email address, or a Social Security number.[86] The COPPA statute also includes within the definition ''any other identifier that the Commission determines permits the physical or online contacting of a specific individual.'' [87]

a. Biometric Data

The Commission proposes using its statutory authority to expand the Rule's coverage by modifying the Rule's definition of ''personal information'' to include ''[a] biometric identifier that can be used for the automated or semi-automated recognition of an individual, including fingerprints or handprints; retina and iris patterns; genetic data, including a DNA sequence; or data derived from voice data, gait data, or facial data.'' [88] The Commission believes this proposed modification is necessary to ensure that the Rule is keeping pace with technological developments that facilitate increasingly sophisticated means of identification.

The majority of comments addressing the question of whether to expand the Rule's definition of ''personal information'' supported the addition of biometric data.[89] These commenters asserted that different types of biometric data can be used to contact specific individuals. For example, a coalition of consumer groups recommended adding biometric data, including genetic data, fingerprints, and retinal patterns, to the Rule's enumerated list of ''personal information.'' [90] These commenters cited consumer products' current use of biometrics to identify and authenticate users through such mechanisms as fingerprints and face scans.[91] They also noted that while some types of personal information may be altered to protect privacy, biometric data collected today may be used to identify and contact specific children for the rest of their lives.[92] Several other commenters also argued that the permanent and unalterable nature of biometric data makes it particularly sensitive.[93] Additional commenters noted that many states have expanded the definition of personally identifiable information to include biometric data as have other federal laws and regulations, such as the Department of Education's Family Educational Rights and Privacy Act (''FERPA'') Regulations, 34 CFR 99.3.[94]

A small number of commenters urged the Commission to proceed cautiously with respect to adding biometric data to the Rule's personal information definition. These commenters suggested that such an expansion could stifle innovation [95] or questioned whether biometric data allows the physical or online contacting of a specific individual.[96] Some commenters also

operator from making telephone calls after the operator has obtained consent. Indeed, the definition of ''personal information'' includes a telephone number under COPPA and the COPPA Rule, and neither the statute nor the Rule includes a prohibition on using that information to make telephone calls.

[83] *See* 78 FR 3972 at 3975. At that time, the Commission also questioned whether adding mobile telephone numbers would result in greater convenience for parents in providing consent, noting that children might have difficulty distinguishing between a parent's mobile number and a landline number. *See* 78 FR 3972 at 3975. This concern seems less significant today given that many more consumers now rely exclusively on their mobile phone.

[84] 78 FR 3972 at 3975, citing 76 FR 59804 at 59810.

[85] 15 U.S.C. 6501(12) (providing that ''the term 'online contact information' means an email address or *another substantially similar identifier that permits direct contact with a person online*'' (emphasis added)).

[86] *See* 15 U.S.C. 6501(8).

[87] 15 U.S.C. 6501(8)(F). As part of the 2013 Amendments, the Commission used this statutory authority to add several new identifiers to the COPPA Rule's definition of ''personal information.'' *See* 78 FR 3972 at 3978–83. For example, the Commission added a photograph, video, or audio file containing a child's image or voice, and it also included geolocation information sufficient to identify street name and name of a city or town. Additionally, the Commission added persistent identifiers that can be used to recognize a user over time and across different websites or online services, which the Rule had previously only covered when associated with individually identifiable information. *See* 64 FR 59888 at 59912.

[88] Given that the Rule's definition of ''personal information'' currently includes ''a photograph, video, or audio file where such file contains a child's image or voice,'' the Commission believes facial features, voice, and gait are already covered under the Rule. 16 CFR 312.2, definition of ''personal information,'' paragraph 8. However, in light of the inherently personal and sensitive nature of data derived from voice data, gait data, and facial data, the Commission proposes to cover this data within the proposed list of biometric identifiers.

[89] *See, e.g.,* Attorney General of Arizona, at 2; Joint Attorneys General, at 7; Consumer Reports, at 14; SuperAwesome, at 12; CARU, at 3–5; ESRB, at 5; and kidSAFE, at 6.

[90] Joint Consumer Groups, at 52–53.

[91] *Id.* at 53 (citing Heather Kelly, *Fingerprints and Face Scans Are the Future of Smartphones. These Holdouts Refuse to Use Them,* Wash. Post (Nov. 15, 2019)).

[92] Joint Consumer Groups, at 53.

[93] CARU, at 4; H. Adams, at 3; Joint Attorneys General, at 7, 11–12.

[94] Future of Privacy Forum (''FPF''), at 4–5; D. Derigiotis Burns Wilcox, at 1–2.

[95] The App Association (''ACT''), at 4.

[96] CCIA, at 4; The Toy Association, at 3, 17.

recommended that, if the Commission does define biometric data as personal information, it should consider appropriate exceptions, for example, where the data enhances the security of a child-directed service [97] or the operator promptly deletes the data.[98]

The Commission believes that, as with a photograph, video, or audio file containing a child's image or voice, biometric data is inherently personal in nature. Indeed, the Commission agrees with the many commenters [99] who argued that the personal, permanent, and unique nature of biometric data makes it sensitive, and the Commission believes that the privacy interest in protecting such data is a strong one.

And, as with some facial and voice recognition technologies, the Commission believes that biometric recognition systems are sufficiently sophisticated to permit the use of identifiers such as fingerprints and handprints; retina and iris patterns; genetic data, including a DNA sequence; and data derived from voice data, gait data, or facial data to identify and contact a specific individual either physically or online.

The Commission notes that the specific biometric identifiers that it proposes adding to the Rule's personal information definition are examples and not an exhaustive list. The Commission welcomes further comment on this proposed modification, including whether it should consider additional biometric identifier examples and whether there are appropriate exceptions to any of the Rule's requirements that it should consider applying to biometric data, such as exceptions for biometric data that has been promptly deleted.

b. Inferred and Other Data

In addition to biometric data, the Commission also asked for comment on whether it should expand the Rule's definition of ''personal information'' to include data that is inferred about, but not directly collected from, children, or other data that serves as a proxy for ''personal information.'' Several commenters recommended such an expansion.[100] For example, one commenter stated that inferred data, including predictive behavior, is often incredibly sensitive and that even when it is supplied in the aggregate, can be easily re-identified.[101] The commenter also noted that certain State laws include inferred data in their definitions of personally identifiable information.[102] Another pointed to the ability of analysts to infer personal information that the Rule covers, such as an individual's geolocation, from data that currently falls outside the Rule's scope.[103]

Commenters opposed to including inferred data stated that such an expansion would not be in accordance with the COPPA statute, which covers data collected ''from'' a child.[104] Some commenters opposed to the inclusion of inferred data argued that inferred data does not permit the physical or online contacting of the child.[105] Some commenters also expressed concern that adding inferred data would create ambiguity and hamper companies' abilities to provide websites and online services to children, would stifle new products and services, and may prohibit the practice of contextual advertising.[106]

The Commission has decided not to propose including inferred data or data that may serve as a proxy for ''personal information'' within the definition. As several commenters correctly note, the COPPA statute expressly pertains to the collection of personal information *from* a child.[107] Therefore, to the extent data is collected from a source other than the child, such information is outside the scope of the COPPA statute and such an expansion would exceed the Commission's authority. Inferred data or data that may serve as a proxy for ''personal information'' could fall within COPPA's scope, however, if it is combined with additional data that would meet the Rule's current definition of ''personal information.'' In such a case, the existing ''catch-all'' provision of that definition would apply.[108]

c. Persistent Identifiers

In 2013, the Commission used its authority under 15 U.S.C. 6501(8)(F) to modify the Rule's definition of ''personal information'' to include persistent identifiers that can be used to recognize a user over time and across different websites or online services. Prior to that change, the Rule covered persistent identifiers only when they were combined with certain types of identifying information.[109] As part of the 2019 Rule Review Initiation, the Commission asked for comment on whether this modification has resulted in stronger privacy protections for children. The Commission also asked whether the modification has had any negative consequences.

A number of commenters, citing a variety of reasons, argued that the amendment to include ''stand-alone'' persistent identifiers as personal information was incorrect or had caused harm. Several commenters claimed that persistent identifiers alone do not allow for the physical or online contacting of a child, and thus should not be included unless linked to other forms of personal information.[110] Commenters also argued

[97] The Toy Association, at 3, 17.

[98] kidSAFE, at 6.

[99] *See, e.g.,* Joint Consumer Groups, at 53; CARU, at 3–5; H. Adams, at 3; Joint Attorneys General, at 11–12.

[100] *See, e.g.,* Joint Consumer Groups, at 53–54 (supporting the inclusion of inferred data); London School of Economics, at 1, 9 (supporting the inclusion of inferred data from profiling and other data analytics); SuperAwesome, at 18 (supporting the inclusion of inferred data, health and activity information derived from fitness trackers, and household viewing data from automated content recognition systems in televisions and video streaming devices); C. Frascella, at 2–3 (supporting the inclusion of personal information collected from children through digital reproduction technology); Parent Coalition for Student Privacy, at 5–8 (supporting, among other things, the inclusion of inferred data and proxy data, such as the language spoken at home and the length of time the child has lived in the United States); UnidosUS (''Unidos''), at 5 (urging the Commission to study the use of ''cultural cues'' as personal information). *See also, e.g.,* National Center on Sexual Exploitation, at 2 (expressing general support for expanding the definition of ''personal information'' to protect children).

[101] Parent Coalition for Student Privacy, at 5.

[102] *Id.* (citing Colorado's Student Data Transparency and Security Act and California's Consumer Privacy Act).

[103] Joint Consumer Groups, at 54 (''For example, non-geolocation ambient data collected by a mobile device operating system does not constitute an independently enumerated category of personal information under the current iteration of the COPPA Rule. But a savvy analyst could use data collected by a mobile device to infer specific geolocation or other details that clearly *would* fall under the COPPA Rule definition of personal information'') (emphasis in original).

[104] *See, e.g.,* IAB, at 4; NCTA—The internet and Television Association (''NCTA''), at 5–7; U.S. Chamber of Commerce, at 3. *See also* CCIA, at 4 (asserting that the COPPA Rule already covers the processing of personal information to derive inferences about a specific user and that the use of aggregated data that does not relate to a specific user is outside the scope of the COPPA statute's definition of ''personal information'').

[105] *See, e.g.,* IAB, at 4; The Toy Association, at 16–17.

[106] *See* CIPL, at 2; U.S. Chamber of Commerce, at 3; IAB, at 4; internet Association, at 5–6; PRIVO, at 8.

[107] 15 U.S.C. 6502(a)(1).

[108] *See* 16 CFR 312.2, definition of ''personal information,'' paragraph 10 (defining ''personal information'' to include ''[i]nformation 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'').

[109] *See* 64 FR 59888 at 59912.

[110] *See, e.g.,* TechFreedom, at 8 (''[P]ersistent identifiers on their own can only identify a device, not a 'specific person' as the COPPA statute requires''); Competitive Enterprise Institute, at 2 (''[P]ersistent online identifiers do not 'permit[] the physical or online contacting of a specific individual' in the sense that Congress contemplated when it enacted COPPA in 1998''); ICLE, at 6 (''Neither IP addresses nor device identifiers alone 'permit the physical or online contacting of a specific individual' as required by 15 U.S.C. 6501(8)(F)''); NetChoice, at 3 (''Persistent

that the persistent identifier modification harmed both operators and children. Specifically, some commenters pointed to operators' lost revenue from targeted advertising, which requires collection of persistent identifiers, and the resulting reduction of available child-appropriate content online due to operators' inability to monetize such content.[111] One commenter stated that while the 2013 modification ''served the widely held goal of excluding children from interest-based advertising,'' it created uncertainty for operators' use of data for internal operations.[112] The commenter suggested that the Commission consider exempting persistent identifiers used for internal operations from the Rule's deletion requirements.[113]

In contrast, other commenters expressed strong support for the 2013 persistent identifier modification. For example, while acknowledging that it took time for the digital advertising industry to adapt to the new definition, one commenter described the 2013 modification as ''wholly positive.'' [114] The commenter also noted that the change recognized that unique technical identifiers might be just as personal as traditional identifiers such as name or address when used to contact, track, or profile users.[115] The commenter stated that this change ''laid the groundwork for many countries adopting this expanded definition of personal information in their updated privacy laws.'' [116]

After reviewing the comments relevant to this issue, the Commission has decided to retain the 2013 modification including stand-alone persistent identifiers as ''personal information.'' The Commission is not persuaded by the argument that persistent identifiers must be associated with other individually identifiable information to permit the physical or online contacting of a specific individual. The Commission specifically addressed, and rejected, this argument during its discussion of the 2013 Amendments. There, the Commission rejected the claim that persistent identifiers only permit contact with a device. Instead, the Commission pointed to the reality that at any given moment a specific individual is using that device, noting that this reality underlies the very premise behind behavioral advertising.[117] The Commission also reasoned that while multiple people in a single home often use the same phone number, home address, and email address, Congress nevertheless defined these identifiers as ''individually identifiable information'' in the COPPA statute.[118] The adoption of similar approaches in other legal regimes enacted since the 2013 Amendments further supports the Commission's position.[119]

Nor does the Commission find compelling the argument that the 2013 persistent identifier modification has caused harm by hindering the ability of operators to monetize online content through targeted advertising. One of the stated goals of including persistent identifiers within the definition of ''personal information'' was to prevent the collection of personal information from children for behavioral advertising without parental consent.[120] After reviewing the comments, the Commission has determined that the privacy benefits of such an approach outweigh the potential harm, including the purported harm created by requiring operators to provide notice and seek verifiable parental consent in order to contact children through targeted advertising.[121]

Moreover, it bears noting, as the Commission did in 2013, that the expansion of the personal information definition was coupled with a newly created exception that allows operators to collect persistent identifiers from children to provide support for the internal operations of the website or online service without providing notice or obtaining parental consent. One of these purposes is serving contextual advertising, which provides operators another avenue for monetizing online content. The Commission continues to believe that it struck the proper balance in 2013 when it expanded the personal information definition while also creating a new exception to the Rule's requirements.

3. School and School-Authorized Education Purpose

As discussed in Part IV.C.3.a., the Commission proposes codifying current guidance on ed tech [122] by adding an

identifiers, like cookies, only identify devices—not a person'').

[111] *See, e.g.,* ICLE, at 7–12. These commenters also included content creators on YouTube. *See, e.g.,* Skyship Entertainment; J. Johnston (J House Vlogs); H. and S. Jho (Sockeye Media LLC). *See also* CARU, at 1 (noting that ''[t]he addition of 'persistent identifier' to the definition of 'Personal Information' has resulted in improved privacy protections for children but has had negative consequences for industry, specifically the lack of robust and creative child-directed content''); IAB, at 4 (noting that this modification may have had the unintended effect of reducing the availability of children's online content).

[112] CCIA, at 3.

[113] *Id.*

[114] SuperAwesome, at 18.

[115] *Id. See also* Princeton University Center for Information Technology Policy (''Princeton University''), at 4 (''In the most recent COPPA Rule revision, the FTC recognized that 'persistent identifiers' are a form of 'personal information,' because they enable singling out a specific user through their device for contact. This makes sense; we see no basis in computer science for treating persistent identifiers any differently from other means of directing communications, such as telephone numbers or email addresses. While the technical details differ, the use of the information is the same'').

[116] SuperAwesome, at 18. This commenter also recommended that the Commission expand the ''personal information'' definition's non-exhaustive list of persistent identifiers to include ''device ID, [a]dvertising ID or similar'' IDs and a ''user agent or other device information which, when combined, can be used to create a unique fingerprint of the device.'' SuperAwesome, at 17. Because the Rule provides examples of persistent identifiers rather than an exhaustive list, the Commission does not find it necessary to include these elements within the definition.

[117] 78 FR 3972 at 3980.

[118] *Id.* (citing 15 U.S.C. 6501(8)).

[119] *See* The European Union's General Data Protection Regulation (''GDPR''), which defines ''personal data'' as ''any information relating to an identified or identifiable natural person . . . [A]n identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as . . . an online identifier.'' GDPR, Article 4, *available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434.* Recital 30 of the GDPR notes that ''natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as [I]nternet [P]rotocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags.'' Recital 30, *available at https://eur-lex.europa.eu/eli/reg/2016/679.* The California Privacy Rights Act similarly defines ''personal information'' as ''information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household,'' and includes identifiers such as online identifiers. Section 3, Title 1.81.5 of the CCPA, added to Part 4 of Division 3 of the California Civil Code § 1798.140(v). This approach is also consistent with the FTC's own precedent. *See Protecting Consumer Privacy in an Era of Rapid Change,* Federal Trade Commission (March 2012), available at *https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326bprivacybreport.pdf; FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising* (February 2009), available at *https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.*

[120] 78 FR 3972 at 3979–3981.

[121] The Commission received comments from content creators who indicated that the 2013 Amendments resulted in the loss of the ability to monetize content through targeted advertising. *See* Skyship Entertainment; J. Johnston (J House Vlogs); H. and S. Jho (Sockeye Media LLC). As discussed in Part IV.A.2.c., the 2013 Amendments permit monetization through other avenues, such as contextual advertising, or through providing notice and seeking parental consent for the use of personal information for targeted advertising.

[122] *Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act,* Federal Trade Commission (May 19, 2022), available at

Continued

exception for parental consent in certain, limited situations in which a school authorizes an operator to collect personal information from a child. The Commission also proposes adding definitions for ''school'' and ''school-authorized education purpose,'' terms that are incorporated into the functioning of the proposed exception and necessary to cabin its scope. Part IV.C.3.a. provides further discussion about these definitions.

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

As discussed in Part IV.A.2.c., the 2013 Amendments expanded the definition of ''personal information'' to include stand-alone persistent identifiers ''that can be used to recognize a user over time and across different websites or online services.'' [123] The 2013 Amendments balanced this expansion by creating an exception to the Rule's notice and consent requirements for operators that collect a persistent identifier for the ''sole purpose of providing support for the internal operations of the website or online service.'' [124] The Rule defines ''support for the internal operations of the website or online service'' to include a number of specified activities and provides that the information collected to perform those activities cannot be used or disclosed ''to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose.'' [125]

A variety of commenters recommended modifying the definition of ''support for the internal operations of the website or online service.'' Multiple consumer and privacy advocates, academics, and one advertising platform called for the Commission to define ''support for the internal operations'' narrowly and thereby restrict the exception's use.[126] For example, a coalition of consumer groups argued that the current definition is overly broad, too vague, and allows operators to avoid or minimize their COPPA obligations.[127] These commenters cited the lack of clarity between data collection for permissible content personalization versus collection for impermissible behavioral advertising.[128] To prevent operators from applying the exception too broadly, the coalition recommended a number of modifications to the definition, including limiting ''personalization'' to user-driven actions and to exclude methods designed to maximize user engagement.[129]

Several commenters specifically recommended that the Commission exclude the practice of ''ad attribution''—which allows the advertiser to associate a consumer's action with a particular ad—from the support for the internal operations definition.[130] A group of State Attorneys General argued that ad attribution is unrelated to the activities enumerated in the definition and that the practice ''necessarily involves 'recogniz[ing] a user over time and across different [websites] or online services.' '' [131] Another commenter argued that companies should not be able to track children across online services to determine which ads are effective because the harm to privacy outweighs the practice's negligible benefit.[132]

In contrast, many industry commenters recommended that the Commission expand the list of activities that fall under the support for the internal operations definition. With respect to ad attribution, these commenters generally cited the practical need of websites and online services that monetize through advertising to evaluate the effectiveness of ad campaigns or to measure conversion in order to calculate compensation for advertising partners.[133] Some commenters characterized the practice as common and expected, and they argued that reducing the ability to monetize would result in the development of fewer apps and online experiences for children.[134]

Several commenters stated that ad attribution already falls within the definition but supported a Rule modification to make this clear.[135] One argued that the definition's prohibition on the collection of persistent identifiers for behavioral advertising ''serves as a safeguard to assure that [attribution] is appropriately limited.'' [136]

Commenters also recommended that a number of other practices should fall within the definition of ''support for the internal operations of the website or online service.'' These include additional ad measuring techniques,[137] different types of personalization activities,[138] product improvement,[139] and fraud detection.[140]

https://www.ftc.gov/legal-library/browse/policy-statement-federal-trade-commission-education-technology-childrens-online-privacy-protection; ComplyingwithCOPPA:FrequentlyAskedQuestions (''*COPPA FAQs*''), *FAQ Section N,* available at *https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.*

[123] 16 CFR 312.2, definition of ''personal information,'' paragraph 7.

[124] 16 CFR 312.5(c)(7).

[125] 16 CFR 312.2, definition of ''support for the internal operations of the website or online service.'' The definition includes activities such as those necessary to maintain or analyze the functioning of a site or service; personalize content; serve contextual advertising or cap the frequency of advertising; and protect the security or integrity of the user, site, or service.

[126] Joint Consumer Groups, at 48–52; S. Egelman, at 5–6 (stating that, from a technical standpoint, persistent identifiers are not needed to carry out the activities listed in the support for the internal operations of the website or online service definition); Princeton University, at 5–7 (expressing reservations about the scope of the internal operations exception); SuperAwesome, at 5–7 and 19–20 (noting that the industry-standard persistent identifiers are not needed for most internal operations and that the support for the internal operations exception should be significantly narrowed, if not eliminated).

[127] Joint Consumer Groups, at 48–52.

[128] *Id.* at 48–49.

[129] *Id.* at 50–52.

[130] Joint Attorneys General, at 8; Joint Consumer Groups, at 51–52; Consumer Reports, at 14–15.

[131] Joint Attorneys General, at 8.

[132] Consumer Reports, at 14–15 (noting that it is unclear whether companies are following COPPA's existing restraints on operators' use of the support for the internal operations exception).

[133] ESA, at 17–18; CARU, at 5; The Toy Association, at 14–15; NCTA, at 10. *See also* Committee for Justice, at 4.

[134] *See, e.g.,* kidSAFE, at 6.

[135] *See, e.g.,* The Toy Association, at 14–15; NCTA, at 10; ESA, at 18; CARU, at 5. *See also* PRIVO, at 8 (noting that ''the Commission should make clear whether attribution and remarketing can be claimed to be support for internal operations'').

[136] The Toy Association, at 15.

[137] *See, e.g.,* ANA, at 11 (recommending including click/conversion tracking, ad modeling, and A/B testing, practices that provide operators with information about the value of their ads, reduce the need for behavioral targeted ads, and allow operators to determine the most ''user-friendly'' version of a site); Google, at 17 (recommending adding conversion tracking and ad modeling, which allow measuring the relevance and appropriateness of ads); IAB, at 3 (recommending including conversion tracking and advertising modeling because they ''are fundamental activities that improve the customer and business experience without creating additional privacy risks to children''); internet Association, at 6–7 (recommending including click/conversion tracking and ad modeling support because they ''support child-centered content creation and, in each case, can be undertaken without focusing on a specific child's behavior over time for targeting purposes'').

[138] *See, e.g.,* NCTA, at 9–10 (recommending including user-driven and user-engagement personalization to allow, for example, ''activities to tailor users' experiences based on their prior interactions with a site or service (whether derived from predictive analytics, real-time behaviors, or both)''); Viacom, at 3 (requesting the Commission clarify that the definition includes ''enhanced personalization techniques based on operator-driven first-party metrics and inferences about user interaction''); CCIA, at 5–6 (recommending including personalization to a user, such as ''the recommendation of content based on prior activity on the website or online service'').

[139] *See, e.g.,* ANA, at 11; kidSAFE, at 7; Khan Academy, at 2–3 (noting that it is important to preserve the operator's ability to use data for educational research, product development, and to analyze the functioning of a product).

[140] *See, e.g.,* SIIA, at 5 (recommending amending (1)(v) of the definition to ''[p]rotect the security or

By expanding the definition of ''personal information'' to include stand-alone persistent identifiers, while at the same time creating an exception that allowed operators to collect such identifiers without providing notice and obtaining consent for a set of prescribed internal operations, the Commission struck an important balance between privacy and practicality in the 2013 Amendments.[141] After careful consideration of the comments that addressed the Rule's support for the internal operations definition, the Commission does not believe that significant modifications to either narrow or expand the definition are necessary.

With respect to ad attribution, which generated significant commentary, the Commission believes the practice currently falls within the support for the internal operations definition. When it amended the definition in 2013, the Commission declined to enumerate certain categories of uses, including payment and delivery functions, optimization, and statistical reporting, in the Rule, stating that the definitional language sufficiently covered such functions as activities necessary to '' 'maintain or analyze' the functions'' of the website or service.[142] The Commission believes that ad attribution, where a persistent identifier is used to determine whether a particular advertisement led a user to take a particular action, falls within various categories, such as the concept of ''payment and delivery functions'' and ''optimization and statistical reporting.'' When used as a tool against click fraud, ad attribution also falls within the category of ''protecting against fraud or theft,'' an activity that served as a basis for the Commission's creation of the support for the internal operations exception.[143] That said, as the definition makes clear, the Commission would not treat ad attribution as support for the internal operations of the website or online service if the information collected to perform the activity is 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.'' [144]

The definition's use restriction is an important safeguard to help ensure that operators do not misuse the exception that allows them to collect a persistent identifier in order to provide support for the internal operations without providing notice and obtaining consent.[145] 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. To increase transparency and to help ensure that operators follow the use restriction, the Commission proposes modifying the online notice requirements in § 312.4(d) to require any operator using the support for the internal operations exception to specifically identify the practices for which the operator has collected a persistent identifier and the means the operator uses to comply with the definition's use restriction.[146]

With respect to the other proposed additions, the Commission does not believe additional enumerated activities are necessary. Other proposed additions—such as personalization, product improvement, and fraud prevention—are already covered.[147] As the Commission noted in developing the 2013 Amendments, the Commission is cognizant that future technical innovation may result in additional activities that websites or online services find necessary to support their internal operations.[148] Therefore, the Commission reminds interested parties that they may utilize the process permitted under § 312.12(b) of the Rule, which allows parties to request Commission approval of additional activities to be included within the support for the internal operations definition based on a detailed justification and an analysis of the activities' potential effects on children's online privacy.

Although the Commission does not find it necessary to modify the definition's enumerated activities, it does propose modifications to the definition's use restriction. Currently, the use restriction applies to each of the seven enumerated activities in the definition, and it states that information collected for those enumerated activities may not 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.[149] However, certain of these activities likely necessarily require an operator to contact an individual, for example in order to ''[f]ulfill a request of a child as permitted by §§ 312.5(c)(3) and (4).'' [150] Therefore, the Commission proposes clarifying language to indicate that the information collected for these enumerated activities may be used or disclosed to carry out the activities permitted under the support for the internal operations exception.

In addition, the Commission proposes expanding its non-exhaustive list of use restrictions. The Commission agrees with commenters who argued that the support for the internal operations exception should not be used to allow operators to maximize children's engagement without verifiable parental consent. Therefore, the Commission proposes prohibiting operators that use this exception from using or disclosing personal information in connection with processes, including machine learning processes, that encourage or prompt use of a website or online service. This proposed addition prohibits operators from using or disclosing persistent identifiers to optimize user attention or maximize user engagement with the website or online service, including by sending notifications to prompt the child to engage with the site or service, without verifiable parental consent.

The Commission welcomes comment on whether there are other engagement

integrity of the user, [website], or online service of the operator or its service providers''). *See also* kidSAFE, at 7 (recommending expanding the definition to include customer or technical support, market research and user surveys, demographic analysis, ''or any other function that helps operate internal features and activities offered by a site or app'').

[141] *See* 78 FR 3972 at 3980 (noting that ''the Commission recognizes that persistent identifiers are also 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 user's experience'').

[142] *Id.* at 3981.

[143] 76 FR 59804 at 59812; 77 FR 46643 at 46647–46648.

[144] 16 CFR 312.2, definition of ''support for the internal operations of the website or online service,'' paragraph 2. This restriction applies to each of the activities enumerated in the definition.

[145] 16 CFR 312.5(c)(7).

[146] *See* Part IV.B.3. for further discussion of these proposed changes.

[147] *See, e.g.,* 77 FR 46643 at 46647 (noting that ''[b]y carving out exceptions for support for internal operations, the Commission stated it intended to exempt from COPPA's coverage the collection and use of identifiers for authenticating users, improving site navigation, maintaining user preferences, serving contextual advertisements, protecting against fraud or theft, or otherwise personalizing, improving upon, or securing a [website] or online service'').

[148] 78 FR 3972 at 3981.

[149] 16 CFR 312.2, definition of ''support for the internal operations of the website or online service,'' paragraph 2.

[150] 16 CFR 312.2, definition of ''support for the internal operations of the website or online service,'' paragraph (1)(vii). For example, § 312.5(c)(3) allows an operator to ''respond directly on a one-time basis to a specific request from the child.'' The Commission notes that the exceptions set forth in §§ 312.5(c)(3) and (4) are limited to responding to a child's specific request. Such a response would not include contacting an individual for another purpose, including through behavioral advertising, amassing a profile on a specific individual, or for any other purpose.

techniques the Rule should address. The Commission also welcomes comment on 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 service.

5. Website or Online Service Directed to Children

The Commission proposes a number of changes to the definition of ''website or online service directed to children.'' Overall, the Commission does not intend these proposed changes to alter the definition substantively; rather, the changes will provide additional insight into and clarity regarding how the Commission currently interprets and applies the definition.

a. Multi-Factor Test

The first paragraph of the definition sets forth a list of factors the Commission will consider in determining whether a particular website or online service is child-directed. The Commission received a significant number of comments regarding the Rule's multi-factor test. Several industry commenters encouraged the FTC to continue relying on a multi-factor test to determine whether a site or service is directed to children, balancing both context (*e.g.,* intent to target children, promoted to children, and empirical evidence of audience) and content (*e.g.,* subject matter, animation, and child-oriented activities) factors.[151] These commenters discouraged the FTC from relying on a single factor taken alone, arguing that a multi-factor evaluation allows flexibility and takes into account that some factors may be more or less indicative than others.[152]

At the same time, commenters also recommended that the Commission reevaluate the test's existing factors, claiming that some are outdated and no longer seem indicative of child-directed websites or online services. For example, several industry members noted that content styles such as animation are not necessarily determinative of whether a service is child-directed.[153] In addition, several industry members recommended that the FTC consider giving more weight to particular factors when determining whether a website or online service is directed to children or that it create a sliding scale for existing factors to provide more guidance for operators.[154] For example, a number of commenters recommended that the Commission weigh more heavily operators' intended audience as opposed to empirical evidence of audience composition.[155]

Several FTC-approved COPPA Safe Harbor programs suggested adding new factors to the Rule to help guide operators, including by adding an operator's self-categorization to third parties. One such program, for example, recommended considering marketing materials directed to third-party partners or advertisers, claiming that such materials can provide insights on the operator's target and users.[156] Another supported consideration of ''whether an operator self-categorizes its website or online service as child-directed on third[-]party platforms.'' [157] A third FTC-approved COPPA Safe Harbor program recommended requiring operators to periodically analyze the demographics of their audience or users and to consider consumer inquiries and complaints.[158]

Some commenters cautioned against relying on an operator's internal rating system or a third party's rating system as a factor.[159] One such commenter argued that relying on operators' internal rating systems would potentially punish those that engage in good faith, responsible review activities and might violate section 230 of the Communications Decency Act.[160] The commenter also argued that a third party's ratings do not constitute competent and empirical evidence regarding audience composition or evidence regarding the intended audience, and further argued that relying on such ratings increases an operator's risk of unexpected liability, particularly if the rating system may have been developed for a purpose unrelated to the COPPA Rule's factors.[161]

The Commission continues to believe that the Rule's multi-factor test, which applies a ''totality of the circumstances'' standard, is the most practical and effective means for determining whether a website or online service is directed to children. The determination of whether a given site or service is child-directed is necessarily fact-based and requires flexibility as individual factors may be more or less relevant depending on the context. Moreover, a requirement that the Commission, in all cases, weigh more heavily certain factors could unduly hamper the Commission's law enforcement efforts. For example, it is

[151] *See, e.g.,* Google, at 15 (''By equally balancing both content and context factors in applying the multi-factor test, operators—including creators, developers and platforms—are less likely to be over- or under-inclusive in making determinations about child-directed services, particularly when decisions are being made at the margins. We are concerned that pulling out a single factor as a litmus test for child-directedness can lead to bad outcomes, resulting in the application of COPPA obligations to general audience content where it doesn't make sense to apply the same protections we'd apply to children's services''); internet Association, at 9 (''The Commission should continue to consider these factors holistically, with no single factor taking precedence over others. Reliance on a comprehensive multi-factor test that includes audience composition as one of many factors balances both content and context inputs and provides the flexibility needed to apply the Rule in the context of new technology and evolving platforms such as interactive media'').

[152] *See, e.g.,* internet Association, at 9; CIPL, at 3–4; Google, at 15–16; Pokémon Company International, Inc. (''Pokémon''), at 1–2; ESA, at 3–8. *See also* TechFreedom, at 19 (''The FTC should reinforce its prior decision to apply a 'totality of circumstances' test in determining whether content is child-directed'').

[153] *See, e.g.,* ANA, at 8 (noting that animated content is often adult-oriented rather than child-oriented); Pokémon, at 2 (noting that popular adult animated content such as ''Family Guy'' or ''South Park'' illustrates that the use of animation is no longer a clear indicator that the use of animated characters is targeted to children); ESA, at 6 (asserting that the use of animated characters should not be given weight in video game and similar media contexts because video games are computer-generated media and therefore inherently utilize animated characters).

[154] *See, e.g.,* Pokémon, at 2 (suggesting ''weighting'' the factors); TRUSTe, LLC (''TRUSTe''), at 2 (noting that, while not dispositive, audience composition and target market factors will have a higher likelihood of determining that the service is child-directed); SuperAwesome, at 11 (suggesting the establishment of a roadmap for the Rule's scope to evolve from ''content-based'' to ''user-based'' factors, noting that ''[t]oday, the best (and highly imperfect) method for determining whether a user is a child is by categori[z]ing the content being accessed, *e.g.* is it child-directed or not. In the near future, new technologies will make it possible to identify whether a user is a child on any website or app, and without collecting more personal information to verify age'').

[155] *See, e.g.,* ANA, at 8; J. Johnston (J House Vlogs), at 14; The Toy Association, at 10. *See also generally* Screen Actors Guild-American Federation of Television and Radio Artists (''SAG–AFTRA''), at 4–5 (asserting that, when applying the COPPA Rule to content creators who distribute their content on general audience platforms, the Commission should consider the content creators' knowledge and intent).

[156] TRUSTe, at 1–2.

[157] kidSAFE, at 7 (also recommending the addition of ''video content'' to the existing factor of ''music or other audio content'').

[158] CARU, at 6–7 (suggesting that such factors would be particularly relevant to sites or services that were not originally directed to children, but where the audience has reached a threshold level such that COPPA protections should apply).

[159] *See, e.g.,* ANA, at 8; ESRB, at 7.

[160] ANA, at 8 (stating that ''Section 230 of the Communications Decency Act explicitly states that no provider of an interactive computer service shall be held liable for 'any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable.' As such, considering content moderation actions taken by companies to oversee content on their platforms as a basis for liability may be impermissible pursuant to the Communications Decency Act'').

[161] ANA, at 8–9.

not hard to envision operators circumventing the Rule by claiming an ''intended'' adult audience despite the attributes and overall look and feel of the site or service appearing to be directed to children.[162] Additionally, a rigid approach that prioritizes specific factors is unlikely to be nimble enough to address a site or service that changes its characteristics over time.

The Commission does not propose eliminating any of the existing factors or modifying how it applies the multi-factor test.[163] However, the Commission proposes modifications to clarify the evidence the Commission will consider regarding audience composition and intended audience.

Specifically, the Commission proposes adding a non-exhaustive list of examples of evidence the Commission will consider in analyzing audience composition and intended audience. The Commission agrees with those commenters that argued that an operator's marketing materials and own representations about the nature of its site or service are relevant. Such materials and representations can provide insight into the operator's understanding of its intended or actual audience and are thus relevant to the Commission's analysis. Additionally, the Commission believes that other factors can help elucidate the intended or actual audience of a site or service, including user or third-party reviews and the age of users on similar websites or services. Therefore, the Commission proposes adding ''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'' as examples of evidence the Commission will consider. Because many of these examples can provide evidence as to both audience composition and intended audience, the Commission also proposes a technical fix to remove the comma between ''competent and reliable empirical evidence regarding audience composition'' and ''evidence regarding the intended audience.''

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

The second paragraph of the definition of ''website or online service directed to children'' states ''[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.'' [164] The Commission added this language in 2013, along with parallel changes to the definition of ''operator,'' in order ''to allocate and clarify the responsibilities under COPPA'' of third parties that collect information from users of child-directed sites and services.[165] The changes clarified that the child-directed content provider is strictly liable when a third party collects personal information through its site or service, while the third party is liable only if it had actual knowledge that the site or service from which it was collecting personal information was child-directed.[166]

Because the second paragraph of this definition specifies that the operator must have actual knowledge that it is collecting personal information ''directly'' from users of another site or service, the Commission is concerned that entities with actual knowledge that they receive large amounts of children's data from another site or service that is directed to children, without collecting it directly from the users of such site or service, may avoid COPPA's requirements. For example, the online advertising ecosystem involves ad exchanges that receive data from an ad network that has collected information from users of a child-directed site or service. In the same spirit of avoiding a loophole that led the Commission to amend the Rule in 2013, the Commission proposes modifying the current language by deleting the word ''directly.'' The Commission did not seek comment in the 2019 Rule Review Initiation on this aspect of the Rule's definition of ''website or online service directed to children'' and therefore welcomes comment on this proposed modification.

c. Mixed Audience

The 2013 Amendments established a distinction between child-directed sites and services that target children as a ''primary audience'' and those for which children are one of multiple audiences—so called ''mixed audience'' sites or services. Specifically, the Rule provides that a website or online service that meets the multi-factor test for being child-directed ''but that does not target children as its primary audience, shall not be deemed directed to children'' so long as the operator first collects age information and then prevents the collection, use, or disclosure of information from users who identify as younger than 13 before providing notice and obtaining verifiable parental consent.[167] This allows operators of mixed audience sites or services to use an age-screen and apply COPPA protections only to those users who are under 13.

Although there appears to be general support for the mixed audience classification, a number of commenters cited confusion regarding its application and called on the Commission to provide additional clarity on where to draw the line between general audience, primarily child-directed, and mixed audience categories of sites and services.[168] One commenter noted that the mixed audience definition is confusing and the language ''shall not be deemed directed to children''

[162] Indeed, the Commission has previously acknowledged that a website or online service with the attributes, look, and feel of a property targeted to children would be deemed directed to children even if an operator claims that was not the intent. 78 FR 3972 at 3983.

[163] With respect to animation as a factor, the Commission recognizes that a variety of adult content uses animated characters. By the same token, animation can be an important characteristic of child-directed sites and services. Accordingly, as with the other enumerated factors, animation continues to be one of several potentially relevant considerations the Commission will take into account in determining whether a specific site or service is directed to children.

[164] 16 CFR 312.2, definition of ''website or online service directed to children,'' paragraph 2.

[165] 78 FR 3972 at 3975. The 2013 Amendments added a proviso to the definition of ''operator'' discussing the circumstances under which personal information is collected or maintained on behalf of an operator. *See* 16 CFR 312.2, definition of ''operator.''

[166] The Commission stated that ''for purposes of the [COPPA] statute'' the third party ''has effectively adopted that child-directed content as its own and that portion of its service may appropriately be deemed to be directed to children.'' 78 FR 3972 at 3978.

[167] 16 CFR 312.2, definition of ''website or online service directed to children,'' paragraph 3.

[168] *See, e.g.,* ANA, at 9 (''Although the ability to age screen users has helped businesses ascertain those users to which COPPA applies, children could benefit from the FTC providing additional guidance on the threshold for determining whether a website or online service is *primarily* directed to children''); Google, at 13 (''We support the retention of the mixed audience category, which appropriately recognizes that it is reasonable to treat age screened users as adults when the underlying child-directed content is also directed to adult audiences . . . At the same time, we believe that the definition of mixed audience as currently drafted requires significant clarification, especially with respect to its distinction from primarily child-directed and general audience content''); Lego, at 7 (''[F]urther clarity on how content for mixed audience and adults could be interpreted by regulatory and self-regulatory authorities would increase our ability to provide clearer direction internally on content development''); The Toy Association, at 9 (suggesting the Commission amend the Rule ''to establish that a mixed audience site or service, including apps or platforms, is one that offers content directed to children, but whose target audience likely includes a significant number of tweens, teens or adults'') (bold typeface omitted); Internet Association, at 7 (''While it can be fairly straightforward to identify sites and services that are directed primarily to children, the concept of mixed audience sites is not clearly defined and the implications of this concept are unclear and unpredictable'').

suggests that such sites or services are not within the definition of child-directed websites or online services.[169] Others recommended the Commission use a specific threshold for making the determination or provide additional guidance based on the Rule's multi-factor test.[170]

Commenters also questioned the effectiveness of age screening, with some arguing that children have been conditioned to lie about their age in order to circumvent age gates.[171] Others expressed support for the current approach,[172] and some warned against specifying proscriptive methods for age screening, as it could prevent companies from innovating new methods.[173]

Through the 2013 Amendments, the Commission intended mixed audience sites and services to be a subset of the ''child-directed'' category of websites or online services to which COPPA applies. A website or online service falls under the mixed audience designation if it: (1) meets the Rule's multi-factor test for being child-directed; and (2) does not target children as its primary audience. Unlike other child-directed sites and services, mixed audience sites and services may collect age information and need only apply COPPA's protections to those users who identify as under 13. An operator falling under this mixed audience designation may not collect personal information from any visitor until it collects age information from the visitor. To the extent the visitor identifies themselves as under age 13, the operator must provide notice and obtain verifiable parental consent before collecting, using, and disclosing personal information from the visitor.[174]

To make its position clearer, the Commission proposes adding to the Rule a separate, stand-alone definition for ''mixed audience website or online service.'' This definition provides that a mixed audience site or service is one that meets the criteria of the Rule's multi-factor test but does not target children as the primary audience.[175]

The proposed definition also provides additional clarity on the means by which an operator of a mixed audience site or service can determine whether a user is a child. First, the Commission agrees with the comments that recommend it allow operators flexibility in determining whether a user is a child. To that end, the proposed definition allows operators to collect age information or use ''another means that is reasonably calculated, in light of available technology, to determine whether the visitor is a child,'' reflecting a standard used elsewhere in the Rule.[176] Although currently collecting age information may be the most practical means for determining that a user is a child, the proposed definition allows operators to innovate and develop additional mechanisms that do not rely on a user's self-declaration.[177]

Additionally, consistent with long-standing staff guidance,[178] the proposed mixed audience definition specifically requires that the means used for determining whether a visitor is a child ''be done in a neutral manner that does not default to a set age or encourage visitors to falsify age information.'' This, for instance, would prevent operators from suggesting to users that certain features will not be available for users who identify as younger than 13.

To further clarify the obligations of an operator of a mixed audience site or service, the Commission also proposes amending paragraph (3) of the definition of ''website or online service directed to children'' by stating that such operators shall not be deemed directed to children with regard to any visitor not identified as under 13.

B. Notice (16 CFR 312.4)

The Commission proposes a number of modifications to the Rule's direct notice and online notice provisions.

1. Direct Notice to the Parent (Paragraph (b))

Section 312.4(b) requires operators to make reasonable efforts to ensure that parents receive direct notice of an operator's practices with respect to the collection, use, or disclosure of children's information. The Commission proposes adding references to ''school'' in § 312.4(b) to cover the situation in which an operator relies on authorization from a school to collect information from a child and provides the direct notice to the school rather than to the child's parent. As discussed in Part IV.C.3.a., the Commission is proposing to add an exception to the Rule's parental consent requirement where an operator, in limited contexts, obtains authorization from a school to collect a child's personal information. For purposes of authorization, ''school'' includes individual schools as well as local educational agencies and State educational agencies, as those terms are defined under Federal law.[179]

Just as notice is necessary for a parent to provide informed and meaningful consent, a school must also obtain information about an operator's data

[169] kidSAFE, at 7–8 (''How can a site or service be 'directed to children' for purposes of the factors' test, yet not be 'deemed directed to children' for purposes of compliance?'').

[170] *See, e.g.,* The Toy Association, at 9 (''[The Toy Association] suggests that the FTC consider revising the Rule to establish that a mixed audience site or service, including apps or platforms, is one that offers content directed to children, but whose target audience likely includes a significant number of tweens, teens or adults, even if segments other than children do not comprise 50% or more of the audience'') (bold typeface omitted); CIPL, at 3–4 (''In its application of the COPPA Rule, the Commission has increasingly blurred the lines between services that are 'primarily directed to children,' services that target children as one but not the primary audience ('mixed audience'), and general audience sites that don't target children as an audience. The FTC should issue guidance based upon the multi-factor test in COPPA to ensure that content creators, app developers and platforms understand how the rules apply to their products and services''); SIIA, at 4 (''As the way people consume content online continues to evolve, additional guidance is needed on the line between child-directed and mixed audience services''); ESRB, at 6–7 (recommending the Commission provide clarity on the ''directed to children'' analysis through rulemaking or guidance); and J. Johnston (J House Vlogs), at 16 (requesting an ''[e]mergency [e]nforcement [s]tatement from the FTC providing . . . [c]larity on the lines between child-directed, mixed-audience, and general audience content'').

[171] *See, e.g.,* SuperAwesome, at 21; PRIVO, at 7–8; Joint Attorneys General, at 9; CARU, at 8.

[172] *See, e.g.,* CCIA, at 7–8; U.S. Chamber of Commerce, at 4–5; ANA, at 9; Internet Association, at 9.

[173] *See, e.g.,* CCIA, at 8; ANA, at 9.

[174] 16 CFR 312.2, definition of ''website or online service directed to children,'' paragraph 3.

[175] Current staff guidance notes that operators should carefully analyze the intended audience, actual audience, and, in many instances, the likely audience for the website or online service in determining whether children are the primary audience or not. *COPPA FAQ*s, FAQ D.5.

[176] *Compare* proposed definition of ''mixed audience website or online service'' (as quoted in the text accompanying this footnote) *with* 16 CFR 312.5(b)(1) (''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.'').

[177] Indeed, the Commission supports the development of other means and mechanisms to determine whether the user is a child. Other jurisdictions, such as the United Kingdom, have conducted research that indicates that mechanisms other than self-declaration may be a more effective means of age assurance. Specifically, the research states that parents found the self-declaration method ''easy to circumvent,'' with many parents ''open about themselves and their children lying about their ages.'' *Families' attitudes towards age assurance,* Research commissioned by the United Kingdom's Information Commissioner's Office and Ofcom (Oct. 11, 2022), at 19, available at *https://www.gov.uk/government/publications/families-attitudes-towards-age-assurance-research-commissioned-by-the-ico-and-ofcom.*

[178] *COPPA FAQs,* FAQ D.7.

[179] *See* Part IV.C.3.a. for further discussion on the proposed school authorization exception. This proposed definition is intended to preserve the ability of local and State educational agencies to contract on behalf of multiple schools and school districts. This definition aligns with current staff guidance providing that ''[a]s a best practice, we recommend that schools or school districts decide whether a particular site's or service's information practices are appropriate, rather than delegating that decision to the teacher.'' *COPPA FAQs,* FAQ N.3.

collection and use practices before authorizing collection. Therefore, as part of the proposed school authorization exception, an operator must make reasonable efforts to ensure that the school receives the notice that the operator would otherwise provide to a child's parent.

2. Content of the Direct Notice (Paragraph (c))

Section 312.4(c) details the content of the direct notice required where an operator avails itself of one of the Rule's exceptions to prior parental consent set forth in § 312.5(c)(1)–(8). The Commission proposes several modifications to § 312.4(c). The first is to delete the reference to ''parent'' in the § 312.4(c) heading. This modification is to accommodate the proposed new § 312.4(c)(5), which specifies the content of the direct notice where an operator relies on school authorization to collect personal information.

Next, the Commission proposes modifying language in § 312.4(c)(1) and a number of its paragraphs. As currently drafted, this section sets forth the required content of direct notice when an operator collects personal information in order to initiate parental consent under the parental consent exception listed in § 312.5(c)(1). The Commission proposes revising the heading of § 312.4(c)(1) by adding the phrase ''for purposes of obtaining consent, including . . .'' after ''[c]ontent of the direct notice to the parent'' and before ''under § 312.5(c)(1).'' This change would clarify that this direct notice requirement applies to all instances in which the operator provides direct notice to a parent for the purposes of obtaining consent, including under § 312.5(c)(1).

In its current form, § 312.4(c)(1) presumes that an operator has collected a parent's online contact information and, potentially, the name of the child or parent. However, operators are free to use other means to initiate parental consent, including those that do not require collecting online contact information. For example, an operator could use an in-app pop-up message that directs the child to hand a device to the parent and then instructs a parent to call a toll-free number. The modification is intended to clarify that even where the operator does not collect personal information to initiate consent under § 312.5(c)(1), it still must provide the relevant aspects of the § 312.4(c)(1) direct notice to the parent.

Because the Commission's proposed changes to § 312.4(c)(1) would expand the scope of when an operator must provide this direct notice, the Commission proposes modifications to indicate that §§ 312.4(c)(1)(i) and newly-numbered 312.4(c)(1)(vii) may not be applicable in all instances.[180] Additionally, because §§ 312.4(c)(1)(i) and newly-numbered 312.4(c)(1)(vii) apply to scenarios in which an operator is obtaining parental consent under the parental consent exception provided in § 312.5(c)(1), the Commission proposes making minor modifications to those sections to align language with that exception. Specifically, that exception permits operators to collect a child's name or online contact information prior to obtaining parental consent, and the proposed notice would require the operator to indicate when it has collected a child's name or online contact information.

The Commission also proposes adding a new paragraph (iv) to require that operators sharing personal information with third parties identify the third parties as well as the purposes for such sharing, should the parent provide consent. This new paragraph (iv) will 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 disclosure of such information, except where such disclosure is integral to the nature of the website or online service.[181] For example, such disclosure could be integral if the website or online service is an online messaging forum through which children necessarily have to disclose their personal information, such as online contact information, to other users on that forum. 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. In order to minimize the burden on operators, and to maintain the goal of providing parents with a clear and concise direct notice, the proposed modification allows operators to disclose the categories of third parties with which the operator shares data rather than identifying each individual entity. The Commission welcomes further comment on whether information regarding the identities or categories of third parties with which an operator shares information is most appropriately placed in the direct notice to parents required under § 312.4(c) or in the online notice required under § 312.4(d).

Additionally, the Commission proposes a number of clarifying changes. First, the Commission proposes clarifying that the information at issue in the first clause of § 312.4(c)(1)(ii) is ''personal information.'' [182] Second, in § 312.4(c)(1)(iii), the Commission proposes clarifying that the direct notice must include how the operator intends to use the personal information collected from the child. For example, to the extent an operator uses personal information collected from a child to encourage or prompt use of the operator's website or online service such as through a push notification, such use must be explicitly stated in the direct notice. Additionally, the Commission further proposes to change the current use of ''or'' to ''and'' to indicate that the operator must provide all information listed in § 312.4(c)(1)(iii). Lastly, the Commission also proposes removing the term ''additional'' from § 312.4(c)(1)(iii) because this paragraph no longer applies solely to instances in which the operator collects the parent's or child's name or online contact information.

In addition to the proposed modifications to § 312.4(c)(1), the Commission proposes adding § 312.4(c)(5) to identify the content of the direct notice an operator must provide when seeking to obtain school authorization to collect personal information.[183] While tailored to the school context, the requirements in this new provision generally track the proposed modifications to § 312.4(c)(1).[184]

[180] As discussed in Part IV.B.2., the Commission proposes expanding § 312.4(c)(1) to include instances in which operators collect information other than online contact information to obtain consent. The modifications to §§ 312.4(c)(1)(i) and newly-numbered 312.4(c)(1)(vii) address those instances in which an operator may not have collected a parent's or child's online contact information to obtain consent.

[181] This proposed modification effectuates current requirements under the Rule, namely § 312.5(a)(2), which states that ''[a]n 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.''

[182] This clause currently uses the term ''such information.'' 16 CFR 312.4(c)(1)(ii).

[183] The Commission is aware that ed tech operators may enter into standard contracts with schools, school districts, and other education organizations across the country. This direct notice requirement is not meant to interfere with such contractual arrangements. Operators may employ various methods to meet the proposed direct notice requirement without interfering with the standard contract, such as by appending the direct notice to the contract. *See* Part IV.C.3.a. for further discussion of the direct notice required under this exception.

[184] For instance, proposed § 312.4(c)(5)(iii) requires the operator to provide the information collected from the child, how the operator intends to use such information, and the potential opportunities for disclosure. Similarly, to the extent the operator discloses information to third parties, proposed § 312.4(c)(5)(iv) requires the operator to

Continued

3. Notice on the Website or Online Service (Paragraph (d))

The Commission proposes two additions to the Rule's online notice requirement. These additions pertain to an operator's use of the exception for prior parental consent set forth in § 312.5(c)(7) and the proposed exception set forth in new proposed § 312.5(c)(9).[185] The Commission also proposes certain modifications to the Rule's existing online notice requirements.

First, the Commission proposes adding a new paragraph, § 312.4(d)(3), which would require operators that collect a persistent identifier under the support for the internal operations exception in § 312.5(c)(7) to specify the particular internal operation(s) for which the operator has collected the persistent identifier and describe the means it uses to ensure that it does not use or disclose the persistent identifier to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, in connection with processes that encourage or prompt use of a website or online service, or for any other purpose, except as permitted by the support for the internal operations exception.[186]

Currently, an operator that collects a persistent identifier pursuant to § 312.5(c)(7) is not required to provide notice of the collection. The Commission finds merit in the concerns expressed by some commenters about a lack of transparency in how operators implement the support for the internal operations exception and the extent to which they comply with the exception's restrictions.[187] The Commission believes that the proposed disclosure requirements will provide additional clarity into the use of § 312.5(c)(7), will enhance operator accountability, and will function as an important tool for monitoring COPPA compliance.

Second, as discussed in Part IV.C.3.b., the Commission proposes a new parental consent exception, codifying its law enforcement policy statement regarding the collection of audio files.[188] Consistent with this codification, the Commission also proposes a new § 312.4(d)(4) requiring that an operator that collects audio files pursuant to the new § 312.5(c)(9) exception describe how the operator uses the audio files and to represent that it deletes such files immediately after responding to the request for which the files were collected.

The Commission also proposes a number of other modifications to the Rule's online notice requirements. Specifically, the Commission proposes modifying § 312.4(d)(2) to require additional information regarding operators' disclosure practices and operators' retention policies.[189] As discussed earlier, 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. The Commission notes that the COPPA Rule's online notice provision requires that operators describe how they use personal information collected from children.[190] For example, to the extent an operator uses personal information collected from a child to encourage or prompt use of the operator's website or online service such as through a push notification, such use must be explicitly stated in the online notice. The Commission also proposes adding ''if applicable'' to current § 312.4(d)(3) (which would be redesignated as § 312.4(d)(5)) in order to acknowledge that there may be situations in which a parent cannot review or delete the child's personal information.[191]

Lastly, the Commission proposes to delete the reference to ''parent'' in the § 312.4(d) introductory text. This proposal is to align with the Commission's new proposed direct notice requirement to accommodate the proposed new school authorization exception found in § 312.5(c)(10).

4. Additional Notice on the Website or Online Service Where an Operator Has Collected Personal Information Under § 312.5(c)(10) (New Paragraph § 312.4(e))

The Commission also proposes adding a separate online notice provision applicable to operators that obtain school authorization to collect personal information from children pursuant to the proposed exception set forth in § 312.5(c)(10). These disclosures are in addition to the requirements of § 312.4(d). The Commission believes these proposed disclosures will convey important information to parents regarding the limitations on an operator's use and disclosure of personal information collected under the school authorization exception, and the school's ability to review that information and request the deletion of such information.[192]

C. Parental Consent (16 CFR 312.5)

The verifiable parental consent requirement, in combination with the notice provisions, is a fundamental component of the COPPA Rule's ability to protect children's privacy. The Rule requires operators to obtain verifiable parental consent before they collect, use, or disclose a child's personal information.[193] Operators must make ''reasonable efforts to obtain verifiable parental consent'' and any parental consent method ''must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.'' [194] Although the Rule sets forth a non-exhaustive list of methods that the Commission has recognized as meeting this standard, the Commission encourages operators to develop their own consent mechanisms provided they meet the ''reasonably calculated standard'' required by § 312.5(b)(1). In addition to the enumerated consent mechanisms listed in § 312.5(b)(2), § 312.5(c) provides several exceptions pursuant to which an operator may collect limited personal information without first obtaining parental consent and, in some cases, without providing notice.

The Commission requested comment in its 2019 Rule Review Initiation on the efficacy of the Rule's consent requirements, including whether the Commission should add to the list of approved methods and whether there are ways to encourage the development of new consent methods. The Commission also requested comment on whether the Commission should consider additional exceptions to the consent requirement, including with respect to the collection of audio files

provide the identities or specific categories of such third parties and the purposes for such disclosures.

[185] Given that these proposed disclosures may be longer and somewhat technical in nature, the Commission believes their appropriate location is in the operator's online notice rather than the direct notice.

[186] The Commission also proposes requiring operators to implement a data retention policy as part of the requirements for § 312.10. *See* Part IV.G. for a discussion of this proposed change.

[187] *See* Part IV.A.4. for a discussion of these concerns.

[188] *See* Part IV.C.3.b.

[189] The Commission proposes requiring operators to implement a data retention policy as part of the requirements for § 312.10. *See* Part IV.G. for a discussion of this proposed change.

[190] 16 CFR 312.4(d)(2).

[191] As discussed in Part IV.D., operators utilizing the school authorization exception would not be required to provide parents the rights afforded under § 312.6(a) for information collected under that exception.

[192] The school's ability to review information and request the deletion of such information are addressed in Part IV.D. in connection with the proposed modification to § 312.6.

[193] Operators must also obtain such consent for ''any material change in the collection, use, or disclosure practices to which the parent has previously consented.'' 16 CFR 312.5(a)(1).

[194] 16 CFR 312.5(b)(1).

containing a child's voice and in the educational context where a school authorizes the operator to collect personal information.

The Commission proposes modifying the Rule's consent requirements in a number of ways. First, the Commission proposes requiring the operator to obtain separate verifiable parental consent before disclosing personal information collected from a child. The Commission also proposes modifying the consent method set forth in § 312.5(b)(2)(ii) and incorporating into the Rule two previously approved consent mechanisms submitted through the § 312.12(a) voluntary process. Lastly, the Commission proposes modifying the parental consent exceptions set forth in § 312.5(c)(4), (6), and (7) and adding exceptions for where an operator relies on school authorization and for the collection of audio files that contain a child's voice.

1. General Requirements (Paragraph (a))

Section 312.5(a)(1) provides that an operator must obtain verifiable parental consent before collecting, using, or disclosing personal information from a child. While the Commission does not propose modifications to this paragraph, it seeks to make a clarification. This requirement applies to any feature on a website or online service through which an operator collects personal information from a child. For example, if an operator institutes a feature that prompts or enables a child to communicate with a chatbot or other similar computer program that simulates conversation, the operator must obtain verifiable parental consent before collecting any personal information from a child through that feature. While the Commission is not proposing modifications to this paragraph, it welcomes comment on it.

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.'' The Commission proposes 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.[195] Under the proposed language, operators required to obtain separate verifiable parental consent for disclosures may not condition access to the website or online service on such consent.

In the preamble of the 1999 initial COPPA Rule, the Commission noted that ''disclosures to third parties are among the most sensitive and potentially risky uses of children's personal information. This is especially true in light of the fact that children lose even the protections of [COPPA] once their information is disclosed to third parties.'' [196] The Commission remains concerned about the disclosure of personal information collected from children. Indeed, one commenter noted that ''[c]hildren today face surveillance unlike any other generation—their every movement online and off can be tracked by potentially dozens of different companies and organizations.'' [197]

The Commission believes that information sharing is a pervasive practice. Therefore, the Commission finds it appropriate to provide parents with greater control over the disclosure of their children's information by clarifying that § 312.5(a)(2) requires operators to obtain separate verifiable parental consent for disclosures. This includes disclosure of persistent identifiers for targeted advertising purposes, as well as disclosure of other personal information for marketing or other purposes. The Commission did not seek comment on this particular aspect of the Rule's verifiable parental consent requirements in the 2019 Rule Review Initiation and welcomes comment on this proposed modification.

2. Methods for Verifiable Parental Consent (Paragraph (b))

The Commission received numerous comments related to the methods by which operators can obtain parental consent. Many commenters criticized particular approved parental consent methods. Some characterized the methods as outdated or counterintuitive.[198] Others complained that the methods failed to serve unbanked or low-income families who may lack access to the means to provide consent, such as a credit card.[199] Some commenters suggested that the use of credit card data and government-issued IDs are too privacy-invasive,[200] while one advocate claimed that the current methods are better indicators of adulthood than parenthood.[201]

Commenters also expressed concern that the current methods include too much friction, resulting in significant drop-off during the consent process. Commenters noted that this friction discourages operators from creating services that target children or creates an incentive to limit their collection of personal information to avoid triggering COPPA.[202] Consistent with this view, the Network Advertising Initiative stated that ''[r]ecognizing that verifiable parental consent mechanisms are challenging and expensive to implement, and result in considerable drop-off, the practical reality is that most ad-tech companies simply seek to avoid advertising to children altogether.'' [203] Other commenters warned that cumbersome consent methods can drive children to general audience sites, which may have fewer digital safety and privacy protections in place.[204]

Some commenters suggested modifying existing consent methods or adding new ones. For example, several recommended that the Commission eliminate the need for a monetary transaction when an operator obtains consent through a credit or debit card or an online payment system where the system provides notification of transactions that do not involve a charge.[205] Some recommended

[195] This exception aligns with previous staff guidance, in which FTC staff has stated that operators are not required to provide parents with a separate option to consent to the disclosure of the child's personal information where such disclosures are integral to the site or service. The guidance requires the operators to make clear when such disclosures are integral. *See COPPA FAQs,* FAQ A.1. For example, such disclosure could be integral if the website or online service is an online messaging forum through which children necessarily have to disclose their personal information, such as online contact information, to other users on that forum.

[196] 64 FR 59888 at 59899.

[197] Common Sense Media, at 3.

[198] *See, e.g.,* FOSI, at 4–5 (describing current method of requiring submission by facsimile as outdated, staffing a toll-free number as expensive, and requiring a credit card number for a service that should be free as counter-intuitive); ESA, at 24 (''For example, the collection of a driver's license or credit card in connection with a transaction may appear particularly cumbersome in the context of a free mobile app that does not require registration and that collects and uses only limited types of information within the app'').

[199] *See, e.g.,* internet Association, at 13; CIPL, at 5; Net Safety Collaborative, at 2; Connected Camps, at 2.

[200] *See, e.g.,* P. Aftab, at 12–13; *see also* ESRB, at 8 (noting that parents may be disinclined to provide credit card information unless the operator is a name the parents know and trust).

[201] P. Aftab, at 13.

[202] *See, e.g.,* ESRB, at 8; CIPL, at 4–5; Internet Association, at 13; Connected Camps, at 2–3.

[203] *See* NAI, at 2; s*ee also* Attorney General of Arizona, at 2 (noting that ''. . . the cost of obtaining verifiable parental consent can be unduly burdensome on small businesses, and the consent process can be frustrating for both businesses and parents alike'').

[204] *See, e.g.,* Lego, at 4–5; Net Safety Collaborative, at 2.

[205] *See, e.g.,* ANA, at 12 (''. . . companies should be able to obtain verifiable parental consent by requesting a valid credit card from a parent even if the consent is not obtained in connection with a monetary transaction''); kidSAFE, at 10 (''The FTC

Continued

modifying the Rule to allow for the use of text messages to obtain consent. Those commenters noted that text messages are a common alternative to email for verification purposes and argued that text message-based consent is no weaker than consent initiated through the collection of an email address.[206]

Other commenters called for the Commission to add to the list of approved consent methods. They recommended allowing the use of fingerprint or facial recognition technologies that already exist in parents' mobile devices,[207] voice recognition technology currently used in the online banking context,[208] and a variety of other technologies and tools.[209]

Several commenters recommended that the Commission encourage platforms to participate in the parental consent process.[210] One suggested that platforms could provide notifications to the consenting parent about the intended collection, use, or disclosure of the child's personal information.[211] Another suggested that parents would be more likely to engage with platforms than to provide consent on a service-by-service basis.[212]

Commenters also recommended different procedural steps the Commission could undertake. These include such things as the Commission using its authority to conduct studies on the costs and benefits of different consent methods,[213] streamlining the Rule's current 120-day comment period on applications for new parental consent methods,[214] and convening stakeholder meetings to explore effective solutions.[215]

After reviewing these comments, the Commission continues to believe that the Rule's current approach to verifiable parental consent is appropriate and sound. With respect to the more general concerns that COPPA's consent methods create ''friction,'' the Commission stresses that COPPA requires a balance between facilitating consent mechanisms that are not prohibitively difficult for operators or parents, while also ensuring that it is a parent granting informed consent, rather than a child circumventing the process. In response to commenters indicating that this friction has discouraged operators from creating services or caused operators to change their practices, the Commission welcomes the development of methods that prove less cumbersome for operators while still meeting COPPA's statutory requirements.

As to the more specific criticisms of the approved consent mechanisms set forth in the Rule, the Commission notes that operators are not obligated to use any of those methods.[216] Rather, operators are free to develop and use any method that meets the standard contained in § 312.5(b)(1) and to tailor their approach to their own individual situation.

While it is possible that some of the suggested methods could meet the § 312.5(b)(1) requirement, the Commission does not believe the comments contain sufficient detail or context for it to propose adding these additional consent methods at this time. The Commission welcomes further explanation detailing the necessity and practicality of any recommended new consent method, including how it would satisfy the Rule's requirements. This could come in the form of additional comments or through the voluntary approval process provided in § 312.12(a) of the Rule.

At the same time, the Commission agrees that platforms could play an important role in the consent process, and the Commission has long recognized the potential of a platform-based common consent mechanism.[217] The Commission would also welcome further information on the role that platforms could play in facilitating the obtaining of parental consent. In particular, the Commission would be interested in any potential benefits platform-based consent mechanisms would create for operators and parents and what specific steps the Commission could take to encourage development of such mechanisms.

The Commission also agrees with the recommendation that it modify the Rule to eliminate the monetary transaction requirement when an operator obtains consent through a parent's use of a credit card, debit card, or an online payment system. As one commenter noted, many of these payment mechanisms provide a means for the account holder to receive notification of every transaction, even those that cost no money, such as a free mobile app download.[218] In addition, many operators offer their apps or other online services at no charge. Requiring such operators to charge the parent a fee when seeking consent undercuts their ability to offer the service at no cost. Further, the Commission understands that some consumers might be hesitant to complete consent processes when they will incur even a nominal monetary charge.

In proposing this modification, the Commission notes that it had previously determined that a monetary transaction was necessary for this form of consent.[219] At that time, the Commission reasoned that requiring a monetary transaction would increase the method's reliability because the parent would receive a record of the transaction. This would provide the parent notice of purported consent, which, if improperly given, the parent could then withdraw. Because § 312.5(b)(2)(ii), as proposed to be modified, would still require notice of a discrete transaction, even where there is no monetary charge, the Commission believes this indicia of reliability is preserved. Where a payment system cannot provide notice absent a monetary charge, an operator will not be able to obtain consent through this method.

The Commission also agrees with the recommendation to modify the Rule to allow the use of text messages to obtain consent. As discussed in Part IV.A.1., the Commission believes this is achieved through its proposed modification to the ''online contact information'' definition.[220] Therefore, the Commission does not propose

should consider eliminating the need for a 'monetary' transaction when consent is obtained using a credit card, debit card, or other online payment system that provides notification of each discreet [*sic*] transaction'').

[206] *See* ANA, at 12; The Toy Association, at 4; kidSAFE, at 11.

[207] *See* ESRB, at 8.

[208] *See* Net Safety Collaborative, at 2.

[209] *See, e.g.,* Net Choice, at 12 (recommending the use of a digital certificate that uses public key technology coupled with additional steps to demonstrate that consent is from the parent); Internet Association, at 14 (recommending that the Commission add a mechanism whereby parents log into a preexisting parental account); CTIA, at 2–3 (recommending obtaining consent through the set-up process for services, such as wearables, that collect personal information from children at parents' direction); Yoti, at 12 (recommending the use of age estimation and age verification tools instead of parental consent).

[210] *See, e.g.,* Princeton University, at 9 (noting that mobile operating systems offer linked parent and child accounts and could provide an interface for child accounts to submit consent permission requests to parent accounts).

[211] *See* ACT: The App Association, at 4–5.

[212] *See* ESRB, at 8.

[213] *See* Pokémon, at 3.

[214] *See* CCIA, at 10; SIIA, at 3–4.

[215] *See* Lego, at 5; The Toy Association, at 20; Yoti, at 13.

[216] Indeed, the Commission is aware that many operators will choose not to utilize certain enumerated methods. However, the Commission retains these methods in the Rule in case any operator would like to use these methods.

[217] 78 FR 3972 at 3989–90 (noting that platform-based common consent mechanism could simplify operators' and parents' abilities to protect children's privacy).

[218] kidSAFE, at 10.

[219] *See* 76 FR 59804 at 59819; *see also* 78 FR 3972 at 3987.

[220] *See* Part IV.A.1.

modifying § 312.5(b)(2)(ii) to address this recommendation.

In addition to the modification to § 312.5(b)(2)(ii), the Commission also proposes adding two parental consent methods to § 312.5(b). These methods are knowledge-based authentication and the use of facial recognition technology. The Commission approved both methods pursuant to the § 312.12(a) process created from the 2013 Amendments.[221]

3. Exceptions to Prior Parental Consent (Paragraph (c))

The Commission also received numerous comments regarding possible additional exceptions to the Rule's parental consent requirement. The majority of the commenters addressing this issue focused on whether the Commission should allow schools to authorize data collection, use, and disclosure in certain circumstances rather than requiring ed tech operators to obtain parental consent. A smaller number of commenters addressed whether the Commission should codify in the Rule its existing enforcement policy statement regarding the collection of audio files. In addition, several commenters recommended that the Commission expand the Rule's current one-time use exception.

The Commission proposes creating exceptions for where an operator relies on school authorization and for the collection of audio files that contain a child's voice. The Commission also proposes a modification to § 312.5(c)(7), which relates to the support for the internal operations exception, to align with proposed new requirements.[222] Additionally, Commission proposes a modification to § 312.5(c)(4) to exclude from this exception the use of push notifications to encourage or prompt use of a website or online service. Finally, the Commission proposes technical modifications to § 312.5(c)(6). At this time, the Commission does not propose expanding the Rule's current one-time use exception.

a. School Authorization Exception

In response to the Commission's initial proposed COPPA Rule in 1999, stakeholders expressed concern about how the Rule would apply to the use of websites and online services in schools. Some of these commenters claimed that requiring parental consent to collect students' information could interfere with classroom activities.[223] In response, the Commission noted in the final Rule's preamble ''that the Rule does not preclude schools from acting as intermediaries between operators and parents in the notice and consent process, or from serving as the parents' agent in the process.'' [224] It further stated, ''where an operator is authorized by a school to collect personal information from children, after providing notice to the school of the operator's collection, use, and disclosure practices, the operator can presume that the school's authorization is based on the school's having obtained the parent's consent.'' [225] Since that time, Commission staff has provided additional guidance on this issue through its ''Complying with COPPA: Frequently Asked Questions'' document (''COPPA FAQs''), which specifies that an operator may rely on school consent when it collects a child's personal information provided the operator uses the information for an educational purpose and for ''no other commercial purpose.'' [226] The Commission has since issued a policy statement on COPPA's application to ed tech providers, similarly noting that operators of ed tech that collect personal information pursuant to school authorization are prohibited from using such information for any commercial purpose, including marketing, advertising, or other commercial purposes unrelated to the provision of the school-requested online service.[227]

In recent years there has been a significant expansion of ed tech used in both classrooms and in the home.[228] This expansion, in the form of students' increased access to school-issued computers and online learning curricula, raised questions about ed tech providers' compliance with the Rule as well as calls for additional guidance on how COPPA applies in the school context. Stakeholders also questioned how COPPA obligations relate to those operators subject to FERPA, the federal law that protects the privacy of ''education records,'' and its implementing regulations.[229]

In 2017, the FTC and the Department of Education hosted a workshop on student privacy and ed tech to explore these questions.[230] Through the discussions at the workshop, the Commission gathered information that helped inform the questions posed in the 2019 Rule Review Initiation regarding the application of the COPPA Rule to the education context. The Commission asked whether it should modify the Rule to add an exception to the parental consent requirement where the school provides authorization and, if so, whether the exception should mirror the requirements of FERPA's ''school official exception.'' [231] The Commission also asked for comment on various aspects of a school authorization exception, including how student data could be used, who at the school should be able to provide consent, and notice to parents.[232]

[221] *See Letter to Imperium, LLC* (Dec. 23, 2013) (approval of knowledge-based authentication), available at *https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-grants-approval-new-coppa-verifiable-parental-consent-method/131223imperiumcoppa-app.pdf; Letter to Jest8 Limited (Trading as Riyo)* (Nov. 18, 2015) (approval of facial recognition technology), *available at https://www.ftc.gov/system/files/documents/public_statements/881633/151119riyocoppaletter.pdf.*

[222] *See* Part IV.B.3. for discussion of the Commission's proposed notice requirement under 16 CFR 312.4(d)(3).

[223] *See* 64 FR 59888 at 59903.

[224] *Id.*

[225] *Id.*

[226] *COPPA FAQs,* FAQ N.1.

[227] *Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act,* Federal Trade Commission (May 19, 2022), available at *https://www.ftc.gov/legal-library/browse/policy-statement-federal-trade-commission-education-technology-childrens-online-privacy-protection.*

[228] The closure of schools and in-person learning due to the global COVID–19 pandemic added to this expansion as students shifted to remote education.

[229] FERPA applies to all schools receiving funds from any applicable program of the Department of Education. 34 CFR 99.1. In general, unless an exception applies, parents (or students over 18 years of age) must provide consent for the disclosure of personal information from an education record. 34 CFR 99.30. FERPA provides an exception to its parental consent requirement for ''school officials.'' 34 CFR 99.31. Under this exception, schools do not need to obtain consent to disclose personal information where there is a ''legitimate educational interest.'' In addition, the school must maintain direct control over the information.

[230] *Student Privacy and Ed Tech* (Dec. 1, 2017), available at *https://www.ftc.gov/news-events/events/2017/12/student-privacy-ed-tech.*

[231] The FERPA school official exception allows schools to outsource institutional services or functions that involve the disclosure of education records to contractors, consultants, volunteers, or other third parties, provided that the outside party: ''(1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; (3) Is subject to the requirements in 34 CFR 99.33(a) that the personally identifiable information (PII) from education records may be used only for the purposes for which the disclosure was made, *e.g.,* to promote school safety and the physical security of students, and governing the redisclosure of PII from education records; and (4) Meets the criteria specified in the school or local educational agency's (LEA's) annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records.'' *Who is a ''School Official'' Under FERPA?,* Department of Education, available at *https://studentprivacy.ed.gov/faq/who-%E2%80%9Cschool-official%E2%80%9D-under-ferpa.*

[232] The Commission also asked for comment on deletion rights in the educational context. The issue of the deletion of information collected when a school has provided authorization is discussed in Part IV.D.

i. Whether To Include a School Authorization Exception in the Rule

Numerous commenters representing industry and schools, along with some consumer groups, expressed support for codifying a school authorization exception in the Rule so long as such exception is consistent with FERPA and its implementing regulations. That is, where there is a legitimate educational interest to collect the child's data, the school maintains direct control of the data, and the operator uses the data only as permitted by the school and complies with disclosure limits.[233]

In supporting such an exception, several of these commenters raised concerns that requiring schools to obtain consent from parents would be burdensome and costly for schools.[234] These commenters claimed that the burden would include obtaining parental consent as well as providing curriculum to students whose parents did not consent to the use of the ed tech program.[235]

Commenters also raised concerns about requiring ed tech providers to obtain verifiable parental consent from parents. For example, commenters expressed concern that requiring operators to obtain parental consent would require operators to collect additional personal information from parents, much of which is not necessary to provide the educational service, which contradicts data minimization principles.[236] One commenter argued that requiring parents to consent would lead to ''consent fatigue,'' [237] while another commenter explained that operators often do not have a direct touchpoint with parents that could facilitate the consent process.[238]

The Illinois Council of School Attorneys argued that schools are often in a better position than parents to evaluate ed tech products.[239] They also pointed to privacy protections in the FERPA school official exception including the requirement that the school maintain direct control of the data and the operator use the data for only limited, authorized purposes.[240] Finally, in supporting a school authorization exception, some commenters stated that numerous operators have built up their consent process in reliance on the Commission's existing guidance indicating that COPPA permits schools to provide consent for educational purposes.[241]

However, not all commenters supported a school authorization exception, with several consumer groups, parent organizations, and government representatives raising various concerns.[242] For example, a coalition of consumer groups argued that a COPPA exception aligned with FERPA would not adequately protect children because FERPA fails to provide a clear standard for when a party has a ''legitimate educational interest'' as required by the school official exception. The coalition also claimed that schools fail to adequately inform parents about the use of FERPA's school official exception and that most schools are ill-equipped to properly vet the privacy and security practices of ed tech services.[243] Another advocacy organization cited statistics purportedly showing that schools do not comply with the school official exception.[244]

A number of individual parents also opposed the exception. These individuals emphasized that parents should retain the ability afforded to them under COPPA to provide consent to collect, use, and share their children's data.[245] One parent noted that over 400 ed tech providers had access to her

[233] *See, e.g.,* CIPL, at 6; Net Safety Collaborative, at 3; Illinois Council of School Attorneys, at 1–2; Association of American Publishers, at 5; CCIA, at 11; internet Association, at 14–17; SIIA, at 3; Joint comment of the Consortium for School Networking, Knowledge Alliance, National Association of State Boards of Education, and the State Educational Technology Directors Association (''CoSN''), at 2; National School Boards Association, at 4–5; National Parent Teacher Association, at 2; Joint comment of the AASA, the School Superintendents Association, and the Association of Education Service Agencies, at 1–3; CDT, at 5; Khan Academy, at 2; Google, at 18; Future of Privacy Forum, at 10–12; Lego, at 5–6. Some commenters supported the Commission implementing a school authorization exception within the Rule but did not call for alignment with FERPA's school official exception. *See, e.g.,* ANA, at 13–14; Lightspeed, at 1–2; The Toy Association, at 5, 19–20; 5Rights, at 6.

[234] *See* CDT, at 4 (noting that ''[s]ome schools do not have the resources or the time to ask for consent from parents every time they rely on an educational technology product''); CCIA, at 11 (noting that ''[a]s Ed Tech becomes increasingly prevalent in the classroom, requiring parental consent for every online service used in the classroom would quickly become administratively and practically unwieldy for parents and schools alike, with the resulting consent fatigue decreasing the availability of beneficial technologies and services to all students''); Lightspeed, at 2 (''Seeking explicit, written parental approval for every single use of technology by a student at present is impracticable. Requiring parents to affirmatively approve each student's use of every application would lead to an avalanche of paperwork for parents and school administrators, one that would push schools to shy away from utilizing EdTech solutions in the classroom''); National PTA, at 3 (noting that ''[w]hen student data is collected in support of core curricular functions, National PTA believes that schools should be able to act as parents' agents and consent on parents' behalf. However, not all student data collection meets that standard. Schools use education technology for a broad range of extracurricular, non-essential or optional activities . . . We ask that the FTC clarify when schools may act on behalf of parents, differentiating between technology used in support of schools' essential academic and administrative needs and other, optional uses''); Net Safety, at 3 (urging the Commission to ensure that schools' burden and cost of obtaining parental consent under COPPA not be increased); Illinois Council of School Attorneys, at 2 (noting that ''requiring school districts to obtain verifiable parental consent from all parents/guardians for potentially hundreds of education applications in use in a district would be an enormous and unworkable administrative burden, even for those districts that have more resources available to them'').

[235] *See, e.g.,* National School Boards Association, at 3 (''If school districts are required to get actual parent consent, many districts would be unable to deliver the curriculum to students whose parents have not responded, creating inequities in addition to administrative burdens''); CIPL, at 5 (noting that ''[i]t could also result in administrative burden and classroom disruption for teachers to manage different lesson plans for students whose parents have provided consent and those whose parents have not'').

[236] *See* CIPL, at 5; ANA, at 14; CCIA, at 11.

[237] CCIA, at 11.

[238] ANA, at 13.

[239] Illinois Council of School Attorneys, at 1.

[240] The organization also noted that schools consenting on behalf of parents is consistent with their *in loco parentis* role. Illinois Council of School Attorneys, at 1–2.

[241] *See* ANA, at 13; Association of American Publishers, at 3.

[242] *See, e.g.,* EPIC, at 8–9 (asserting that ''[i]nstead of putting the burden on schools to obtain and provide consent on behalf of parents, which they are unauthorized to do under the Act, the burden should be shifted to operators, who are in a better position to do so given advancements in technology and greater availability of resources, to obtain verifiable parental consent''); Joint Consumer Groups, at 20–30; Unidos, at 6 (noting that ''cash-strapped districts could be preyed upon by bad actors targeting these districts by offering free or low-cost programs to gain a foothold in schools and start collecting children's data. Many of these companies have opaque privacy policies. Inadequately funded school administrators and/or teachers will not likely have the resources to advocate for better protections or do a sufficient review to understand policies, especially in an environment where schools are using countless apps and programs''); Illinois Families for Public Schools, at 2 (noting that ''[p]arental consent is especially important in the case of extremely sensitive student data regarding children's behavior, biometrics, geolocation, disabilities, or health conditions. As such, we disagree firmly with the idea of amending COPPA rules to have a Family Educational Rights and Privacy Act (FERPA)-type exception for school officials to grant consent for the collection and use of a child's data in an educational setting in place of a parent. The school-official exception in FERPA has weakened its protections for disclosure of student data, and this should not be a precedent for modifying or weakening the COPPA Rule''); Joint Attorneys General, at 10–11; Parent Coalition for Student Privacy, at 8 (noting that ''[p]arents' existing rights under COPPA to be informed and provide prior consent to any program collecting data directly from their children under the age of 13 should not be erased or limited simply because their children's use of a commercial operator's service occurs inside the school building or at the direction of a teacher or school administrator''); Senator Markey, et al., at 2 (noting that this type of exception could be ''fundamentally inconsistent with the congressional intent behind COPPA'').

[243] *See* Joint Consumer Groups, at 25–29.

[244] *See* Surveillance Technology Oversight Project (''STOP''), at 3–4.

[245] *See, e.g.,* A. Segur, at 1; F. Bocquet, at 1; M. Murphy, at 1; N. Williams, at 1.

child's data, and that she is unable to understand what information was shared with each provider.[246] These parents noted that school districts should not be able to provide consent to ed tech providers on their behalf,[247] and further noted that including such an exception would weaken COPPA rather than strengthen it.[248]

Another concern raised was that such an exception could ultimately swallow the Rule.[249] For instance, in a joint comment of multiple State Attorneys General, the Attorneys General cited the incredible growth in ed tech and noted the technologies are not cabined to the classroom but are often encouraged to be used by students at home, and sometimes for non-educational purposes. The Attorneys General argued that, because the use of ed tech is often mandatory for students, an exception to COPPA's parental consent requirement would force parents to choose between education and their children's online privacy.[250]

While opposing a school authorization exception, the Parent Coalition for Student Privacy argued that if the Commission decides to create one, its applicability should be limited in scope. Specifically, the Coalition argued that schools should not be able to consent to the collection of particularly sensitive data, such as medical or geolocation information.[251]

After careful consideration of the comments, the Commission proposes codifying in the Rule its long-standing guidance that schools, State educational agencies, and local educational agencies may authorize the collection of personal information from students younger than 13 in very limited circumstances; specifically, where the data is used for a school-authorized education purpose and no other commercial purpose.[252]

When a child goes to school, schools have the ability to act *in loco parentis* under certain circumstances. This is particularly the case when schools are selecting the means through which the schools and school districts can achieve their educational purposes, such as when deciding which educational technologies to use in their classrooms. The Commission finds compelling the concern that requiring parental consent in the educational context would impose an undue burden on ed tech providers and educators alike. As an initial matter, many ed tech providers have relied upon and structured their consent mechanisms based on the Commission's existing guidance. Requiring providers to reconfigure their systems to obtain parental consent directly from parents would undoubtedly create logistical problems that could increase costs and potentially dissuade some ed tech providers from offering their services to schools.[253]

The need for parental consent is also likely to interfere with educators' curriculum decisions. As a practical matter, obtaining consent from the parents of every student in a class often will be challenging, in many cases for reasons unrelated to privacy concerns. In situations where some number of parents in a class decline to consent to their children's use of ed tech, schools would face the prospect of foregoing particular services for the entire class or developing a separate mechanism for those students whose parents do not consent. Because the proposed school authorization exception restricts an operator's use of children's data to a school-authorized education purpose and precludes use for commercial purposes such as targeted advertising, it may ultimately be more privacy-protective than requiring ed tech providers to obtain consent from parents.

Finally, the proposed school authorization exception requires that the ed tech provider and the school have in place a written agreement setting forth the exception's requirements.[254] This includes identifying who from the school may provide consent and attesting that such individual has the authority to provide consent; the limitations on the use and disclosure of student data; the school's control over the use, disclosure, and maintenance of the data; and the operator's data retention policy. Accordingly, the proposed exception incorporates the privacy protections contained in the FERPA school official exception. This exception also builds on FERPA's protections by incorporating the Commission's existing prohibition on the use of student data for non-educational commercial purposes.

ii. Permitted Use of Data Collected Through the School Authorization Exception

Existing staff guidance indicates that, where the school authorizes data collection, an operator may only use children's data for an educational purpose and for no other commercial purpose.[255] However, there has been confusion around the parameters of what constitutes an ''educational purpose'' as opposed to a ''commercial purpose.'' [256] Many of the commenters that support a school authorization exception to parental consent called on the Commission to clarify the permissible uses of data collected under such an exception.[257] In an effort to seek further clarity, commenters suggested specific uses that the Commission should explicitly allow or exclude under the exception.[258]

Among these commenters, there was general agreement that the exception should not permit ed tech providers to use student data for marketing purposes, such as serving personalized advertisements.[259] The comments

[246] A. Segur, at 1.

[247] *See* A. Segur, at 1; F. Bocquet, at 1; M. Murphy, at 1; N. Williams, at 1.

[248] *See, e.g.,* A. Segur, at 1; F. Bocquet, at 1; N. Williams, at 1.

[249] *See* Senator Markey, et al., at 2 (noting that such an exception ''risks opening the door to invasive tracking of children for advertising purposes''); Joint Attorneys General, at 10–11.

[250] Joint Attorneys General, at 10–11.

[251] Parent Coalition for Student Privacy, at 11–12.

[252] The definition for ''school-authorized education purpose'' is discussed in Part IV.A.3. *See* Part IV.B.1. for further discussion about the proposed inclusion of State and local educational agencies within the definition of ''school.''

[253] The Commission also agrees with commenters that noted that obtaining parental consent could require providers to collect additional personal information from parents that they would not collect if the school provides consent.

[254] As noted in Part IV.B.2., the Commission is aware that operators may enter into standard contracts to provide ed tech services. So long as the standard contract meets the elements required under proposed § 312.5(c)(10), operators may continue to utilize such contracts.

[255] *See COPPA FAQs,* FAQ N.1; *Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act,* Federal Trade Commission (May 19, 2022), available at *https://www.ftc.gov/legal-library/browse/policy-statement-federal-trade-commission-education-technology-childrens-online-privacy-protection.*

[256] Additionally, FERPA does not define what a ''legitimate educational interest'' is for purposes of the school official exception. Thus, even if the Commission aligned a COPPA school consent exception with FERPA, the scope of the exception would be unclear.

[257] *See, e.g.,* CCIA, at 11–12; Joint comment of the AASA, the School Superintendents Association, and the Association of Education Service Agencies, at 3–4; Parent Coalition for Student Privacy, at 4–5; Google, at 18.

[258] *See, e.g.,* Joint comment of the AASA, the School Superintendents Association, and the Association of Education Service Agencies, at 4 (advocating for the inclusion of product research and development); Parent Coalition for Student Privacy, at 3 (opposing the use of children's information to advertise, improve a service, or develop a new service); Google, at 18 (noting that a ''commercial purpose'' under COPPA could be aligned with FERPA such that ''. . . certain types of processing are impermissible, such as personalized ads or product placements, but other important activities to support educational services are permitted, like the maintenance, development and improvement of the product, analytics, and personalization of content within the service'').

[259] *See, e.g.,* Princeton University, at 10; 5Rights Foundation, at 5 (''FTC could usefully clarify both the definition of 'educational purposes' for which consent can be sought, and the scope of purposes that are proscribed (including, but not limited to,

Continued

reflected less consensus on the question of whether to allow operators to engage in product improvement or development. Some commenters favored allowing product improvement or development under limited circumstances. For example, Lego recommended that the exception allow operators to use aggregated or anonymized data to improve existing products or develop new products that would benefit students.[260] The 5Rights Foundation similarly noted that, if the Commission were to allow operators to use student data to improve products, the student information must be ''de-identified and de-identifiable,'' cannot be shared with third parties, and must be limited to use for improving educational products only.[261]

In contrast, some commenters strongly opposed allowing product improvement absent verifiable parental consent. For example, EPIC argued that product improvement would allow ed tech vendors ''to create virtual laboratories in schools to study child behavior and further develop commercial products for profit, unbeknownst to parents.'' [262] Others raised similar objections,[263] including parents who stated that the Commission should prohibit the use of student data to improve or develop new products or services.[264]

In discussing the appropriate use of student data, several commenters suggested that the Commission adopt an approach similar to the treatment of activities that fall under the COPPA Rule's definition of ''support for the internal operations of the website or online service.'' This approach would allow ed tech providers to use student data for ''analytics, content personalization, and product development, maintenance, and improvement uses that benefit students and schools'' but not for activities such as personalized marketing.[265]

The Commission believes that it should tailor the proposed school exception narrowly while ensuring its practicality for schools and operators. The Commission agrees with the commenters asserting that the use or disclosure of student data for marketing purposes should fall outside the school authorization exception. Indeed, this view is consistent with staff's guidance that schools can consent to the collection of student data for educational purposes but not for other commercial purposes, such as marketing and advertising.[266]

The Commission also agrees with those commenters recommending that the school authorization exception should allow operators to engage in limited product improvement and development, provided certain safeguards are in place. The Commission believes that allowing providers to make ongoing improvements to the educational services the school has authorized benefits students and educators, and that user data may be necessary to identify and remedy a problem or ''bug'' in a product or service. Therefore, in contrast to general marketing, product improvement and development can be viewed as part of providing an educational purpose rather than engaging in an unrelated commercial practice.

That said, the Commission is mindful of the concerns that allowing such uses, particularly product development, could open the door to ed tech providers exploiting the exception. To address these concerns, the Commission proposes that the Rule's definition of a ''school-authorized education purpose'' include product improvement and development (as well as other uses related to the operation of the product, including maintaining, supporting, or diagnosing the service), provided the use is directly related to the service the school authorized. This would permit operators to improve the service, for example by fixing bugs or adding new features, or develop a new version of the service. An operator may not use the information it collected from one educational service to develop or improve a different service.

The Commission believes that limiting product improvement and development in this way will allow ed tech providers to provide better services while helping to safeguard against the use of student data for non-educational purposes. We also believe that this proposed approach is consistent with the requirement under FERPA's school official exception that a school have a ''legitimate educational interest'' to share personal information without parental consent.

The Commission does not agree with the commenters that recommended aligning the permissible uses of data collected under the school authorization exception with the Rule's support for the internal operations exception. The two exceptions serve different purposes, and the activities within the support for the internal operations definition are generally unnecessary for and unrelated to the provision of an educational purpose.[267]

As an additional protection, the proposed school authorization exception would require operators to

direct marketing, behavioural advertising, and any profiling not necessary to the functioning of the service in question)''); Consumer Reports, at 18 (noting that ''. . . operators seeking consent in the school setting should be prohibited from using the information for marketing''); internet Association, at 16 (''IA strongly supports appropriate limits on online service operators' use of students' personal information and does not believe that online services should be able to rely on school official consent in order to use personal information for marketing purposes''); STOP, at 5 (noting that the Rule '' . . . must also prohibit operators from using students' personal information for marketing or product-improvement purposes''); Google, at 18 (recognizing the need to exclude commercial activities like advertising, including personalized ads and product placement).

[260] Lego, at 6.

[261] 5Rights Foundation, at 6. *See also* Khan Academy, at 3 (noting the distinction between internal use of data for educational product development and disclosure of that data to third parties for commercial purposes); Yoti, at 14 (recommending allowing operators to use student data where the school has provided consent for research and development, broadly defined, so long as protections are in place); Oregon Attorney General, at 3 (if operators are allowed to use data for product improvement, Commission should consider ''whether operators are able to de-identify the personal information, and are able to prevent re-identification of the data'').

[262] EPIC, at 11.

[263] *See, e.g.,* Parent Coalition for Student Privacy, at 11 (''The Commission should ban operators of education technology from using or processing de-identified or identifiable student information to improve existing or to develop or improve new educational or non-educational products and services''); Illinois Families for Public Schools, at 2 (opposing use of student data ''for advertising purposes or to improve or develop new products or services'').

[264] *See, e.g.,* F. Bocquet, at 1; N. Williams, at 1.

[265] *See, e.g.,* CCIA, at 12. *See also* CIPL, at 3 (suggesting that companies be allowed to engage in profiling in the education context in order to provide '''personalized'' curricula); School Superintendents, at 3 (recommending that FTC clarify that ''commercial purposes'' for purposes of school consent exception does not include activities that would fall under the Rule's support for internal operations exception); Google, at 18 (''. . . certain types of processing are impermissible, such as personalized ads or product placements, but other important activities to support educational services are permitted, like the maintenance, development and improvement of the product, analytics, and personalization of content within the service'').

[266] *See COPPA FAQs,* FAQ N.1; *Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act,* Federal Trade Commission (May 19, 2022), available at *https://www.ftc.gov/legal-library/browse/policy-statement-federal-trade-commission-education-technology-childrens-online-privacy-protection.*

[267] The Commission notes that one potential area of overlap between these exceptions is that the support for the internal operations exception allows an operator to personalize content on a website or online service. The Commission recognizes that some degree of personalization will be inherent in providing the ed tech service for which the student data is collected. For example, this can include personalizing curricula or advancing a student who has completed an assignment to the next level or unit in a lesson plan. While such personalization would be a permissible part of providing the service, personalization could not include the marketing of services even if those services were educational in nature.

have a written agreement with the school setting forth the exception's requirements. This written agreement must specify that the ed tech provider's use and disclosure of the data collected under the exception is limited to a school-authorized education purpose as defined in the Rule and for no other purpose. As an extra safeguard to help ensure that ed tech providers are using student data appropriately and to align the exception with FERPA, the required written agreement must specify that the school will have direct control over the provider's use, disclosure, and maintenance of the personal information under the exception. The agreement must also include the operator's data retention policy with respect to personal information collected from children under the school authorization exception.

iii. Who at the school should provide authorization?

In response to the question of who should be able to provide authorization for data collection under the school authorization exception, a wide variety of commenters, including industry, FTC-approved COPPA Safe Harbor programs, school personnel, and the Oregon Attorney General, called for flexibility.[268] For example, while the Illinois Council of School Attorneys recommended against specifying who can provide authorization, it stated that if the Commission decides to do so, it should use general, flexible terminology such as ''employees designated by the school's administration or governing board'' to describe individuals who may provide authorization.[269] The Oregon Attorney General called for flexibility and urged the Commission to be mindful that schools and districts obtain and implement ed tech in different ways.[270] Another commenter, kidSAFE, recommended the Commission permit consent from an adult outside the school environment, including coaches or tutors.[271]

Other commenters supported a more prescriptive approach,[272] with some recommending that the Rule not allow teachers to provide consent.[273] One commenter stated that few teachers are in a position to evaluate which ed tech services are trustworthy, adding that allowing individual teachers to make these decisions prevents school administrators from knowing what products are being used in the classroom.[274] Another recommended requiring that, if schools are allowed to provide consent on behalf of parents, the school or district must have clear and uniform policies for adopting ed tech led by a team of qualified education research, curriculum, and privacy, and technology experts.[275] Similarly, Lego recommended that only duly authorized individuals, such as IT administrators, data protection officers, or chief IT officers, provide consent through a contract with the ed tech provider.[276]

Because the Commission believes it is important to accommodate the different ways schools obtain and implement ed tech, the Commission agrees with the commenters that called for flexibility rather than a ''one size fits all'' approach. At the same time, the Commission recognizes the need for measures to prevent the situation in which a school is unaware of the ed tech services their teachers have consented to on an ad hoc basis. Indeed, staff guidance has previously recommended that consent for ed tech to collect personal information comes from the schools or school districts rather than from individual teachers.[277] To balance the need for flexibility with the need for oversight and accountability, the Commission proposes that the written agreement between the ed tech provider and the school, which the new § 312.5(c)(10) exception would require, identify the name and title of the person providing consent and specify that the school has authorized the person to provide such consent.

iv. Notice to Parents

Many of the commenters supporting a school consent exception recommended that parents receive notice of the ed tech providers the school authorized to collect children's data.[278] Some commenters suggested that the notice to parents come from schools, recommending that the notice be similar to the FERPA annual notification requirement[279] or that schools make information about ed tech providers' information practices available to parents in a public place such as the school district's website.[280]

Other commenters raised concerns about the Commission imposing obligations on schools through the Rule. For example, the Oregon Attorney General expressed concern that allowing an operator to shift notice obligations to schools would potentially shield operators from liability.[281] Instead, the Oregon Attorney General recommended that the Commission require the operator to ''provide notice of its information practices in a manner that is easily accessible to all parents . . . and to inform the school on where parents may find such notice of information practices.''[282] Similarly, the Parent Coalition for Student Privacy recommended that, if the Commission creates an exception for school authorization, it require ed tech providers to dedicate space on their website for notices about the exception and explain how the data will be strictly used for educational purposes and state which third parties can access the data.[283]

The Commission agrees that notice is an important aspect of the proposed school authorization exception. At the same time the Commission agrees with commenters who raised concerns about imposing burdens on schools that may not have sufficient resources to undertake an additional administrative responsibility.[284] To promote transparency without burdening schools, the Commission proposes requiring operators to provide notice. Namely, the Commission's proposed addition of § 312.4(e), discussed earlier in Part IV.B.4., would require an operator that collects personal information from a child under the school authorization exception to include an additional notice on its website or online service noting that: (1) the operator has obtained authorization from a school to collect a child's personal information; (2) that the

[268] *See* internet Association, at 15; ANA, at 13; SIIA, at 3; FOSI, at 5; kidSAFE, at 4; Illinois Council of School Attorneys, at 2; Oregon Attorney General, at 2.

[269] Illinois Council of School Attorneys, at 2.

[270] Oregon Attorney General, at 2 (noting that, in Oregon, some schools contract with educational technology companies through an intragovernmental technology alliance while others do so independently).

[271] kidSAFE, at 4.

[272] *See* P. Aftab, at 8; Common Sense Media, at 8; Parent Coalition for Student Privacy, at 14; Lego, at 6; Privo, at 6; STOP, at 4.

[273] *See* P. Aftab, at 8; Common Sense Media, at 8; Lego, at 6; Privo, at 6; STOP, at 4.

[274] P. Aftab, at 8.

[275] Parent Coalition for Student Privacy, at 14.

[276] Lego, at 7.

[277] *COPPA FAQs,* FAQ N.3.

[278] *See, e.g.,* CDT, at 8; Common Sense, at 11; Consumer Reports, at 17; FPF, at 12; The National PTA, at 3; Lego, at 6.

[279] CDT, at 8.

[280] FPF, at 12.

[281] Oregon Attorney General, at 3.

[282] *Id.*

[283] Parent Coalition for Student Privacy, at 8–9 (also recommending that schools should also be required to link to and post this information as it applies to the specific education technology services the schools choose to utilize).

[284] Moreover, the Commission cannot impose COPPA obligations on schools. COPPA applies to an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child. 15 U.S.C 6502(a)(1); 16 CFR 312.3.

operator will use and disclose the information for a school-authorized education purpose and no other purpose; and (3) that the school may review information collected from a child and request deletion of such information.[285]

b. Audio File Exception

In 2013, the Commission expanded the Rule's definition of ''personal information'' to include ''[a] photograph, video, or audio file where such file contains a child's image or voice.'' [286] Since that time there has been a dramatic increase in the popularity of internet-connected ''home assistants'' and other devices that are voice activated and controlled. This led to inquiries from stakeholders about the Rule's applicability to the collection of audio files containing a child's voice where an operator converts the audio to text and then deletes the audio file. While the Commission determined that the Rule applies to such collection, it recognized the value of using verbal commands to perform search and other functions on internet-connected devices, especially for children who have not yet learned to write or those with disabilities. Accordingly, in 2017, the Commission issued an enforcement policy statement indicating that it would not take action against an operator who, without obtaining parental consent, collects a child's voice recording, provided the operator only uses the audio file as a replacement for written words, such as to effectuate an instruction or request, and the operator retains the recording only for a brief period.[287]

In the 2019 Rule Review Initiation, the Commission asked whether it should modify the Rule to include a parental consent exception based on the enforcement policy statement. The Commission also asked whether such an exception should allow an operator to use de-identified audio files for product improvement and, if so, how long an operator could retain such data. Additionally, the Commission asked whether de-identification of audio files is effective at preventing re-identification.

The vast majority of commenters that addressed the issue recommended the Commission modify the Rule to include a parental consent exception for audio files based on the existing enforcement policy statement.[288] Some of these commenters supported the narrow confines of the current enforcement statement, which requires the collected audio file to serve solely as a replacement for written words and be maintained only until completion of that purpose.[289] A number of other commenters, however, recommended that the Commission adopt a more expansive audio exception. For example, Google noted that many voice actions for internet-connected devices are not a replacement for written words. Because of this, Google recommended that the Commission include an expanded exception that ''covers voice data used to perform a task or engage with a device, as well as to replace written words.'' [290] Others made similar recommendations.[291]

Several commenters argued that where an operator de-identifies the audio file, the exception should allow it to engage in product improvement as well as internal operations such as improving functionality and personalization.[292] Only a few of these commenters discussed the means by which an operator could effectively de-identify audio files. One suggested using the approach set forth in a White House draft privacy law, which would require the operator to alter the data to prevent it from being linked to a specific individual, to commit not to re-identify the data, and to require third-party recipients to similarly commit not to re-identify the data.[293] Another commenter suggested the operator could de-link the audio file from a user's account or device identifier.[294]

The Commission received a small number of comments that opposed adding a consent exception for audio files to the Rule. Arguing against an exception, a group of State Attorneys General characterized recordings of children's voices as biometric data and stated that, as such, they are ''individually-identifying and immutable.'' [295] These commenters also questioned whether operators could effectively and consistently de-identify audio files, pointing to numerous instances in which anonymized data had been re-identified.[296] A coalition of consumer groups argued that the Commission's existing enforcement statement, as structured, effectively protects children's privacy and there is no need to amend the Rule to add an exception.[297] The commenters also stated that if the Commission does add an exception to the Rule, the exception should not permit operators to retain or use collected audio files for product improvement even if the files are de-identified.[298]

Based on the comments overall, the Commission proposes codifying the audio file enforcement statement as an exception to the Rule's parental consent requirement, with one modification. The Commission believes the calls to expand the exception to also include audio files used to perform a task or to

[285] *See* Part IV.B.4. for discussion on this proposed change.

[286] 16 CFR 312.2, definition of ''personal information.''

[287] *Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings,* 82 FR 58076 (Dec. 8, 2017), available at *https://www.ftc.gov/system/files/documents/public_statements/1266473/coppa_policy_statement_audiorecordings.pdf.* The enforcement statement also specified that the operator must provide the notice required by the COPPA Rule and sets forth a number of important limitations on the policy's application.

[288] *See, e.g.,* CIPL, at 6; TechFreedom, at 22; ANA, at 14; CCIA, at 13; CTIA, at 5–6; ESA, at 22–23; Google, at 19; internet Association, at 17–18; NCTA, at 11; U.S. Chamber of Commerce, at 5–7.

[289] FOSI, at 6; FPF, at 5–6; The Toy Association, at 17.

[290] Google, at 19 (noting that a written command is not typically used to play a video or turn on an appliance and that collection of this type of voice data would pose no additional risk as it would still be briefly retained only to complete the requested action).

[291] *Id.; see also, e.g.,* CCIA, at 13 (noting that the exception should apply to voice data generally as emerging technologies may not necessarily use verbal commands as a ''replacement'' for written words); U.S. Chamber of Commerce, at 6 (noting that voice-activated commands may not constitute a replacement for written words).

[292] *See* internet Association, at 17–18 (asserting that the exception should allow use of audio recordings to train and improve voice recognition and understanding systems); ANA, at 15 (noting that the exception should allow operators to use de-identified audio files to improve current products and future products); TechFreedom, at 23 (noting that the exception should allow de-identified audio files to train automatic speech recognition systems); NCTA, at 11 (recommending the Commission allow product improvement as well as improved functionality, personalization or analytics, and customer service). *See also* CTIA, at 6 (recommending that even if data is not de-identified, the exception should allow an operator to retain the data for product improvement, provided it is not combined with other personal information and appropriate safeguards are in place).

[293] See TechFreedom, at 25–26, citing White House, Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015 (Feb. 27, 2015), available at *https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-actof-2015-discussion-draft.pdf.* This approach is based on the Commission's own data de-identification standard. *See Protecting Consumer Privacy in an Era of Rapid Change,* Federal Trade Commission (March 2012), page 22, available at *https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.*

[294] NCTA, at 11.

[295] Joint Attorneys General, at 11–12. *See also* A. Wang, at 2–4 (arguing that parental consent should be required for the collection of children's voice recordings because of the risks of an insecure transfer of data and noting that de-identification is not effective at preventing re-identification).

[296] Joint Attorneys General, at 11–12; A. Wang, at 2–4.

[297] Joint Consumer Groups, at 36–41.

[298] *Id.*

engage with a device have merit. Limiting the proposed exception to circumstances in which the voice data replaces written words would be overly restrictive and unnecessarily prevent its application to a variety of internet-connected services that do not involve written commands. Further, because the proposed exception requires the operator to delete the collected audio file as soon as the command or engagement is completed, this expansion will not create additional risk to children's privacy. Additionally, to the extent an operator collects personal information beyond the audio file—such as a transcript of the audio file in combination with other personal information—the operator could not utilize the audio file exception and would have to afford COPPA's protections to that information.

The Commission, however, does not agree that the exception should allow operators to retain the audio files or to use them for other purposes such as product improvement and internal operations, even if the operator has taken steps to de-identify the data. The Commission agrees that a recording of a child's voice is particularly sensitive given that, like other biometric data, it is personal and unique. Consequently, the privacy risk created by such data potentially falling into the wrong hands and being re-identified exceeds the benefit of allowing broader use. This is especially the case where parents are not provided direct notice or provided the opportunity to consent to such practices.

c. Other Exceptions

The Commission also proposes adding language to the support for the internal operations exception, § 312.5(c)(7), to address the new online notice requirement the Commission proposes.[299] This proposal indicates that an operator that collects information under the support for the internal operations exception must provide information in its online notice regarding its use of the exception. The Commission also proposes technical fixes to § 312.5(c)(6) for clarity purposes. Namely, the Commission proposes changing § 312.5(c)(6)(i) from ''protect the security or integrity of its website or online service'' to ''protect the security or integrity of *the* website or online service'' (emphasis added). The Commission also proposes removing ''be'' in § 312.5(c)(6)(iv) to fix a typographical issue.

In addition, the Commission proposes to modify § 312.5(c)(4) to prohibit operators from utilizing this exception to encourage or prompt use of a website or online service. This proposed addition prohibits operators from using online contact information to optimize user attention or maximize user engagement with the website or online service, including by sending push notifications, without first obtaining verifiable parental consent.[300]

Additionally, several commenters recommended that the Commission expand the Rule's current one-time use exception, § 312.5(c)(3).[301] Specifically, multiple commenters noted that the Commission should expand the types of information collected under this exception to include telephone numbers.[302] A commenter also requested the Commission expand this exception to permit multiple contacts with a child without providing notice and an opportunity to opt out, as required by the multiple contact exception.[303]

As explained earlier in the discussion regarding the definition of ''online contact information,'' the Commission proposes modifying this definition to include a mobile telephone number, provided the operator uses it only to send a text message and not for voice communication, unless and until the operator has obtained the parent's verifiable parental consent.[304] The Commission believes that the proposed revision to the definition of ''online contact information'' addresses commenters' recommendations to permit the use of mobile telephone numbers to contact children under the one-time use exception. However, the Commission stresses that under the proposed definition of ''online contact information,'' operators using a child's mobile telephone number under this exception may only text the child and may not call the child.

Further, the Commission is not persuaded by commenters suggesting that it should expand this exception to permit multiple contacts with a child without offering parents notice and the opportunity to opt out. The COPPA statute envisioned the scenario in which an operator would have to contact a child more than once to respond to a specific request, and Congress included notice and opt-out requirements in association with such scenario.[305] This scenario was codified in the COPPA Rule under the multiple contact exception, § 312.5(c)(4). Commenters' recommendation essentially asks the Commission to remove the multiple contact exception's notice and consent requirements. However, the Commission believes these elements are required by the COPPA statute, and therefore it does not propose such modifications.

D. Right To Review Personal Information Provided by a Child (16 CFR 312.6)

The Commission proposes a new paragraph related to the Commission's proposed school authorization exception.[306] Specifically, the Commission proposes requiring operators utilizing such exception to provide schools with the rights operators currently provide parents under § 312.6(a), namely the right to review personal information collected from a child, refuse to permit operators' further use or future online collection of personal information, and to direct operators to delete such information. Under this proposal, operators utilizing the school authorization exception would not be required to provide such rights to parents for information collected under the exception.

Requiring operators to fulfill requests, such as deletion requests, from each parent could result in schools having to provide different services to different children or forego particular services for the entire class based on the request of an individual parent. To reduce this burden, the Commission proposes this modification. The Commission also proposes deleting the reference to ''parent'' in the § 312.6 heading to account for this modification.

E. Prohibition Against Conditioning a Child's Participation on Collection of Personal Information (16 CFR 312.7)

Section 312.7 of the Rule provides that an operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more

[299] This proposal is discussed in Part IV.B.3.

[300] The Commission acknowledges that the *COPPA FAQs* currently indicate that operators may rely on the multiple contact exception to send push notifications to children without first obtaining verifiable parental consent. *COPPA FAQs,* FAQ J.9. The Commission is aware of recent media reports indicating that children may be overusing online services due to engagement-enhancing techniques. The Commission is concerned about the potential harm from such overuse and therefore deems it important to ensure parents are notified and provide verifiable parental consent before operators use such techniques to further children's engagement with websites and online services.

[301] *See, e.g.,* kidSAFE, at 13; Consumer Technology Association (''CTA''), at 6–7; ESA, at 24–25; NCTA, at 17.

[302] kidSAFE, at 13; CTA, at 6–7; ESA, at 24–25; NCTA, at 17.

[303] kidSAFE, at 13.

[304] This discussion can be found in Part IV.A.1.

[305] 15 U.S.C. 6502(b)(2)(C); 64 FR 59888 at 59902.

[306] *See* Part IV.C.3.a. for further discussion of the proposed school authorization exception.

personal information than is reasonably necessary to participate in such activity.

The Commission notes that this provision serves as an outright prohibition on collecting more personal information than is reasonably necessary for a child to participate in a game, offering of a prize, or another activity. Therefore, operators may not collect more information than is reasonably necessary for such participation, even if the operator obtains consent for the collection of information that goes beyond what is reasonably necessary.

With respect to the scope of § 312.7, the Commission is considering adding new language to address the meaning of ''activity,'' as that term is used in § 312.7. Specifically, the Commission is considering including language in § 312.7 to provide that an ''activity'' means ''any activity offered by a website or online service, whether that activity is a subset or component of the website or online service or is the entirety of the website or online service.'' It welcomes comment on whether this language is consistent with the COPPA statute's text and purpose, and it also welcomes comment on whether this change is necessary given the breadth of the plain meaning of the term ''activity.''

F. Confidentiality, Security, and Integrity of Personal Information Collected From Children (16 CFR 312.8)

Section 312.8 of the Rule provides:

The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information from children. The operator must also take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of such information, and who provide assurances that they will maintain the information in such a manner.

In the 2019 Rule Review Initiation, the Commission asked whether operators have implemented sufficient safeguards to protect the personal information they collect from children. The Commission also asked whether the requirements of § 312.8 are adequate and whether the Rule should include more specific data security requirements.

Many commenters asked the Commission to clarify or strengthen operators' obligations under this section. For example, a coalition of consumer groups criticized the Commission for not promulgating clear data security regulations as directed by the COPPA statute.[307] These commenters recommended that the Commission elaborate on the meaning of ''reasonable procedures to protect the confidentiality, security, and integrity'' of children's information.[308] Similarly, an FTC-approved COPPA Safe Harbor program recommended that the Commission provide detailed guidance about minimum standards for what constitutes ''reasonable procedures,'' to help guide operators and FTC-approved COPPA Safe Harbor programs tasked with ensuring that companies are compliant with the Rule.[309]

Some commenters argued that recent data breaches in all industries demonstrate the need for stricter data security requirements for children's personal information.[310] Other commenters expressed a more narrow concern that the evolving online landscape in schools, combined with an increase in data breaches and ransomware attacks, suggests the need for stricter data security requirements for children's personal information generally.[311] In contrast, a small number of commenters opined that operators are adequately protecting children's personal information. For example, the Internet Association stated that the increase in well-publicized breaches has heightened operators' awareness of their obligations and encouraged them to safeguard personal data.[312]

Commenters on both sides—those who believe operators are adequately protecting children's personal information and those who believe operators need to do more—recommended against adding prescriptive data security requirements or risk management controls in the Rule. These commenters expressed concern that such measures could become quickly outdated. For example, the Internet Association and The Toy Association expressed concerns that specific, detailed security requirements and risk management controls might prevent operators from keeping pace with evolving technology and security threats.[313] The internet Association opined that the Rule's flexibility permits operators to develop privacy and security risk management frameworks that are tailored to their activities and users, and that also keep pace with technology, evolving security threats, and varying security risks.[314] FTC-approved COPPA Safe Harbor program kidSAFE and a technology trade association recommended that the Commission keep the ''broad and flexible'' standard in § 312.8 for similar reasons.[315] A group of State Attorneys General also supported a flexible approach.[316] These commenters urged the Commission to proceed cautiously and make clear that any additional data security requirements within the Rule are simply illustrative examples of what constitutes ''reasonable procedures'' rather than an exhaustive list.[317] Such an approach, they argued, would encourage operators to consistently monitor and update security protocols that evolve with ''rapid advances in technology and the enterprising nature of cybercriminals.'' [318]

kidSAFE also encouraged the Commission to consider the varying

[307] *See* Joint Consumer Groups, at 54–56 (criticizing the Commission for neglecting to promulgate regulations that ''require the operator of such a website or online service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children,'' but only adding ''small sections'' about releasing data to third parties in § 312.8 and about data retention and deletion in § 312.10).

[308] *Id.* at 56 (requesting the Commission, in particular, clarify operators' obligations to protect the ''confidentiality'' of children's personal information).

[309] CARU, at 10 (noting that, in its experience, companies make good-faith efforts to establish and maintain reasonable procedures but could use additional guidance about ''minimum standards,'' such as encryption).

[310] *See e.g.,* Consumer Reports, at 24 (listing examples of data breaches and suggesting that the Commission provide ''sufficient enforcement'' to incentivize companies to better steward children's personal information).

[311] Parent Coalition for Student Privacy, at 4 (recommending that the Commission strengthen the Rule's data security requirements generally, in light of the increase in data breaches of schools, school districts, and their vendors); *see also* CoSN, at 2, 4–5 (asking the Commission to strengthen the Rule's security requirements generally, considering the increase of cyberattacks on school districts and citing CoSN's 2019 leadership survey report identifying cybersecurity as the first priority for school system technology administrators).

[312] Internet Association, at 20 (''With the emergence of other privacy and security requirements and fall-out from well-publicized breaches, operators are increasingly aware of their obligations to safeguard personal data about users of any age by maintaining physical, technical, and administrative security procedures that are reasonable and appropriate in light of the nature of the data to be protected'') (footnote omitted). *See also* P. Aftab, at 10 (stating that the ''over-arching principles'' of COPPA's data security guidelines are ''working well,'' although they may require updating and closer examination).

[313] Internet Association, at 20; The Toy Association, at 22 (expressing concerns that specific data security requirements could become quickly outdated and might add costs to operators who must also comply with security requirements in other laws, such as the GDPR and State data security laws).

[314] Internet Association, at 20.

[315] kidSAFE, at 16; *see also* Consumer Technology Association, at 19 (opining that ''[f]lexible, dynamic approaches to security are the best answer to solving the security challenges of both today and tomorrow'').

[316] Joint Attorneys General, at 14–15.

[317] *Id.*

[318] *Id.* at 14.

levels of resources and bargaining power that different operators hold. kidSAFE claimed that smaller companies often lack the resources to invest in their own data security measures or the bargaining power to obtain security assurances from the third-party service providers they use.[319] An individual commenter expressed similar concerns that additional data security requirements might further burden small businesses, which already may not be in a position to determine whether service providers are capable of the Rule's existing security requirements.[320]

In enacting COPPA, Congress recognized the need for heightened protections for children's personal information, and the Commission has long recognized a similar need.[321] The Commission agrees that the proliferation of data breaches in all industries, including schools, supports strong and effective data security requirements, especially for particularly sensitive information like children's data. The Commission also agrees that operators would benefit from additional clarity and detail regarding the Rule's security requirements set forth in § 312.8.

For these reasons, the Commission proposes modifications to the Rule's security requirements. Specifically, the Commission proposes to split the operator's requirements in § 312.8 into discrete paragraphs and provide further guidance as to steps operators can take to comply with each requirement. The second paragraph will provide more guidance on the ''reasonable procedures'' that an operator must establish and maintain under newly-numbered § 312.8(a) to protect the confidentiality, security, and integrity of personal information from children. The third paragraph will address the ''reasonable steps'' an operator should take to release children's personal information only to those capable of protecting such and who provide written assurances to protect the information.

First, the Commission proposes modifying § 312.8 to specify that operators must, at minimum, establish, implement, and maintain a written comprehensive security program that contains safeguards that are appropriate to the sensitivity of children's information and to the operator's size, complexity, and nature and scope of activities. This requirement is modeled on the Commission's original Safeguards Rule implemented under the Gramm-Leach-Bliley Act (''GLBA''), which provides heightened protections for financial institutions' customer data.[322]

To provide additional guidance, the proposed § 312.8 security program must contain a number of specific elements including designating an employee to coordinate the information security program; identifying and, at least annually, performing additional assessments to identify risks to the confidentiality, security, and integrity of personal information collected from children; designing, implementing, and maintaining safeguards to control any identified risks, as well as testing and monitoring the effectiveness of such safeguards; and, at least annually, evaluating and modifying the information security program.

The Commission believes that these modifications are appropriate for several reasons. First, this approach provides additional guidance to operators and FTC-approved COPPA Safe Harbor programs, while also maintaining the Rule's flexibility by allowing for technological advancements and taking into account an operator's size, complexity, and the nature and scope of its activities. It is also consistent with prior Commission COPPA and data security decisions and guidance.[323]

In addition to the proposed written data security program, the Commission also proposes adding language to § 312.8 to clarify that operators that release personal information to third parties or other operators must obtain written assurances that the recipients will employ reasonable measures to maintain the confidentiality, security, and integrity of the information. In 2013, when the Commission amended § 312.8 to require operators to ''take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner,'' the Commission envisioned that operators would obtain assurances ''by contract or otherwise.'' [324] The Commission based this requirement on a similar obligation of financial institutions under the GLBA, which requires entities to ''requir[e] your service providers *by contract* to implement and maintain such safeguards'' (emphasis added).[325] While the Commission expanded on the GLBA's provision to allow operators to obtain assurances by contract ''or otherwise,'' the Commission did not intend to allow operators to rely on verbal assurances alone. Rather, the Commission envisioned other written assurances for which there is tangible evidence, such as a written email or a service provider's written terms and conditions.

Accordingly, the Commission proposes inserting ''written'' to clarify that the assurances operators must obtain from other operators, service providers, and third parties to whom the operator releases children's personal information, or who collect such on the operator's behalf, must be in writing. As similarly noted in the Rule review that led to the 2013 Amendments,[326] this provision is intended to address security issues surrounding business-to-business releases of data. The Commission did not seek specific comment on this aspect of the Rule's security requirements and therefore welcomes comment on this proposed modification.

G. Data Retention and Deletion Requirements (16 CFR 312.10)

Section 312.10 of the Rule currently states that ''an operator of a website or online service shall retain personal information collected online from a child for only as long as is reasonably

[319] kidSAFE, at 15 (opining that it believes operators are implementing sufficient security safeguards considering their varying sizes).

[320] K. O'Connell, at 2.

[321] *See, e.g.,* then-FTC Chairman Robert Pitofsky, FTC Testimony before Senate Committee on Commerce, Science & Transportation, U.S. Senate ''Protection of Children's Privacy on the World Wide Web,'' Sept. 23, 1998, at 4 (testifying in support of enacting COPPA and describing safety concerns that the disclosure of children's personal information may lead to, as pedophiles and other sexual predators use online services to identify and contact children), *available at https://www.ftc.gov/public-statements/1998/09/prepared-statement-federal-trade-commission-protection-childrens-privacy; see also* then-FTC Chairman Jon Leibowitz, ''Updated FTC COPPA Rule,'' Dec. 19, 2012, at 6 (explaining that while COPPA covers only ''a small sliver of the internet'' it is ''an important sliver, a small, Congressionally-mandated oasis sheltering personal privacy, one in which websites must respect the privacy of the most vulnerable and precious among us''), *available at https://www.ftc.gov/public-statements/2012/12/statement-ftc-chairman-jon-leibowitz-updated-coppa-rule-prepared-delivery.*

[322] Safeguards Rule, Final Rule, 67 FR 36484 (May 23, 2002), *available at https://www.ftc.gov/sites/default/files/documents/federal_register_notices/standards-safeguarding-customer-information-16-cfr-part-314/020523standardsforsafeguardingcustomerinformation.pdf.*

[323] *See, e.g., In re Retina-X Studios, LLC,* File No. 172 3118 (2020), *available at https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3118-retina-x-studios-llc-matter; United States* vs. *Unixiz, Inc., et al.,* No. 5:19–cv–2222 (N.D. Cal. 2019), *available at https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3002-unixiz-inc-doing-business-i-dressupcom.*

[324] 78 FR 3972 at 3995.

[325] 16 CFR 314.4(f)(2) (requiring financial institutions to obtain contracts with service providers to implement and maintain safeguards).

[326] 76 FR 59804 at 59821.

necessary to fulfill the purpose for which the information was collected.'' This section further states that ''the operator must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.''

In 2013, the Commission amended the Rule to add the data retention and deletion requirements of § 312.10 pursuant to its 15 U.S.C. 6502(b)(1)(D) authority to establish regulations requiring operators to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. At that time, the Commission explained that timely deletion of data is an integral part of a reasonable data security strategy, referencing the Institute for Public Representation's comment that without such ''operators have no incentive to eliminate children's personal information and may retain it indefinitely.'' [327] The Commission, however, rejected requests to specify a finite timeframe in which companies must delete data, instead deciding to choose ''the phrases 'for only as long as is reasonably necessary' and 'reasonable measures' to avoid the very rigidity about which commenters opposing this provision complain.'' [328]

Although the Commission did not specifically seek comment on data deletion in its 2019 Rule Review Initiation, many of the commenters that recommended the Commission provide more guidance on the § 312.8 requirements also suggested that the Commission clarify operators' obligations under § 312.10. These commenters expressed concern that, without specific time limits on data retention, operators could read the Rule to allow indefinite retention of children's personal information. For example, a group of State Attorneys General asked the Commission to modify the Rule to require operators or others maintaining children's data to serve contextual ads to delete such information immediately at the end of a user's session.[329] Many consumer groups and individual commenters also opined that an increase in school data breaches and ransomware attacks indicates a need for stronger data deletion requirements within the Rule generally.[330] A few commenters asked specifically for data retention limits for personal information stored within the education system or by ed tech providers.[331] Similarly, a non-profit privacy organization requested that the Commission make it clear that operators cannot retain student data indefinitely.[332]

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.

Given the misunderstanding identified by the consumer groups, the Commission now proposes to modify this section to state more explicitly operators' duties with regard to the retention of personal information collected from children. Specifically, the Commission proposes clarifying that operators may retain personal information for only as long as is reasonably necessary for the specific purpose for which it was collected, and not for any secondary purpose. For example, if an operator collects an email address from a child for account creation purposes, the operator could not then use that email address for marketing purposes without first obtaining verifiable parental consent to use that information for that specific purpose. Additionally, the operator must delete the information when such information is no longer reasonably necessary for the purpose for which it was collected.[333] In any event, personal information collected from a child may not be retained indefinitely.

The Commission also proposes requiring an operator to, at least, establish and maintain a written data retention policy specifying its business need for retaining children's personal information and its timeframe for deleting it, precluding indefinite retention.

These proposed modifications are intended to reinforce section 312.7's data minimization requirements, which prohibit an operator 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.[334] Namely, these proposed modifications require that an operator must have a specific business need for retaining information collected from children, and may retain such information for only so long as is reasonably necessary for the specific purpose for which it was collected, and not for any secondary purpose. The modifications also preclude operators from retaining such information indefinitely. The Commission welcomes comment on its proposed modification to this section.

H. Safe Harbor (16 CFR 312.11)

The 2019 Rule Review Initiation posed a number of questions related to the Rule's safe harbor program provision, including: whether it has been effective in enhancing compliance with the Rule; whether the Commission should modify the criteria currently enumerated in § 312.11(b) for approval of FTC-approved COPPA Safe Harbor programs; whether the Commission should clarify or modify § 312.11(g) with respect to the Commission's discretion to initiate an investigation or bring an enforcement action against an operator participating in an FTC-approved COPPA Safe Harbor program; whether the Commission should consider changes to the safe harbor monitoring process, including to promote greater transparency; and whether the Rule should include factors for the Commission to consider in revoking approval for an FTC-approved COPPA Safe Harbor program.

A number of commenters expressed support for the Rule's safe harbor program.[335] At the same time, however,

[327] 78 FR 3972 at 3995.

[328] 78 FR 3972 at 3995, note 302 (rejecting the Institute for Public Representation's request to require companies to delete children's personal information within three months).

[329] Joint Attorneys General, at 8.

[330] Parent Coalition for Student Privacy, at 4 (recommending that the Commission incorporate stronger security standards in the Rule generally, considering the increase in data breaches of schools, school districts, and their vendors, including strengthening COPPA's requirements for data minimization and deletion); CoSN, at 4–5 (recommending that, in light of the growing number of cyberattacks on school districts, the Commission strengthen the Rule's security requirements generally and citing CoSN's 2019 leadership survey report identifying cybersecurity as the first priority for school system technology administrators, including ''efforts to promote transparency, and strengthen data retention and deletion policies'').

[331] *See, e.g.,* Illinois Families for Public Schools, at 2 (asking the Commission to have COPPA adopt Illinois' State law approach that retention of student data must be purpose driven and minimized); D. Derigiotis Burns Wilcox, at 2 (requesting the Commission adopt mandatory limits on the period for retaining personal information stored within the educational system and affiliated vendors).

[332] FPF, at 12.

[333] *See* Compl., *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* (alleging that Amazon.com. Inc. and Amazon.com Services LLC violated § 312.10 by retaining children's personal information longer than was reasonably necessary to fulfill the purposes for collecting the information).

[334] 16 CFR 312.7.

[335] *See, e.g.,* CARU, at 11; SuperAwesome, at 31; PRIVO, at 8; FOSI, at 6; CIPL, at 7. *But see, e.g.,* S. Egelman, at 4–5 (stating the belief that FTC-approved COPPA Safe Harbor programs certify

multiple commenters recommended that the Commission enhance oversight of, and transparency regarding, the safe harbor program by modifying the criteria for the Commission's approval of FTC-approved COPPA Safe Harbor programs' guidelines and the Rule's requirements for FTC-approved COPPA Safe Harbor programs to submit reports to the Commission and retain records.[336] While the Commission continues to believe that FTC-approved COPPA Safe Harbor programs serve an important function in helping companies comply with COPPA, it finds merit in the recommendations for enhanced oversight and transparency. Accordingly, the Commission proposes revisions to § 312.11 of the Rule as set forth in this part of the preamble, which it believes will further strengthen the COPPA Rule's safe harbor program.

1. Criteria for Approval of Self-Regulatory Program Guidelines (§ 312.11(b))

Paragraph 312.11(b) of the Rule requires that FTC-approved COPPA Safe Harbor programs demonstrate that they meet certain performance standards, specifically: (1) requirements to 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 FTC-approved COPPA Safe Harbor program's guidelines; and (3) disciplinary actions for subject operators' non-compliance with self-regulatory program guidelines.

Several commenters recommended that the Commission provide additional clarity regarding the criteria the Commission applies when determining whether to approve an FTC-approved COPPA Safe Harbor program's self-regulatory guidelines. One FTC-approved COPPA Safe Harbor program suggested that the Commission consider publishing a standard set of program requirements, assessment questionnaires, and technical tests for all FTC-approved COPPA Safe Harbor programs to utilize with their subject operators.[337] Another recommended that the FTC consider enumerating minimum operating standards for FTC-approved COPPA Safe Harbor programs, including how often they monitor subject operators' sites and communicate with subject operators.[338] Another commenter recommended that the Commission should require FTC-approved COPPA Safe Harbor programs to apply a duty of care to promote principles behind COPPA when they conduct safe harbor program audits and certifications.[339]

The Commission finds merit in the overall call for additional clarity regarding its criteria for approving FTC-approved COPPA Safe Harbor programs' self-regulatory guidelines. As discussed previously, the Commission proposes changes to the Rule's security requirements.[340] These proposed modifications provide additional guidance on the ''reasonable procedures'' that an operator must establish and maintain to protect the confidentiality, security, and integrity of personal information from children. FTC-approved COPPA Safe Harbor programs can utilize that guidance in determining whether subject operators meet the Rule's § 312.8 requirements.

Further, in parallel with the proposed changes to § 312.8 discussed in Part IV.F., the Commission proposes to revise § 312.11(b)(2) to state explicitly that an FTC-approved COPPA Safe Harbor program's assessments of subject operators must include comprehensive reviews of both the subject operators' *privacy and security* policies, practices, and representations. The Commission does not propose any revisions to § 312.11(b)(1).

2. Reporting and Recordkeeping Requirements (§ 312.11(d) and § 312.11(f))

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 an FTC-approved COPPA Safe Harbor program's guidelines, records of disciplinary actions taken against subject operators, and results of the FTC-approved COPPA Safe Harbor program's § 312.11(b)(2) assessments.

Several commenters recommended that the Commission modify the reporting and recordkeeping requirements in order to strengthen the Commission's oversight of FTC-approved COPPA Safe Harbor programs and to make that oversight more transparent. One commenter recommended that the Commission require FTC-approved COPPA Safe Harbor programs to submit more detailed and frequent reports.[341] Another suggested that the Rule should require such programs to demonstrate on a periodic basis that they are regularly assessing and updating their programs to comply with COPPA.[342]

The Commission agrees with commenters' general recommendation to enhance FTC-approved COPPA Safe Harbor programs' reporting requirements in order to strengthen oversight. Accordingly, the Commission proposes revising § 312.11(d)(1) to require the following additions to the FTC-approved COPPA Safe Harbor programs' annual reports.

First, the Commission proposes requiring FTC-approved COPPA Safe Harbor programs to identify each subject operator and all approved websites or online services in the program, as well as all subject operators that have left the program.[343] The proposed revision further requires an FTC-approved COPPA Safe Harbor program to provide: a narrative description of the program's business model, including whether it provides additional services to subject operators, such as training; copies of each consumer complaint related to each subject operator's violation of an FTC-approved COPPA Safe Harbor program's guidelines; and a description of the process for determining whether a subject operator is subject to discipline (in addition to the existing requirement to describe any disciplinary action that the FTC-approved COPPA Safe Harbor program took against any

online services that do not comply with the Rule and that, if the COPPA statute permitted the Commission to do so, it would be better for the Commission to eliminate the safe harbor program); Joint Consumer Groups, at 15–20 (arguing that the safe harbor program does not effectively protect children's privacy because of online services' low participation rates, a lack of sufficiently strict requirements for approval of safe harbor programs, and a lack of safe harbor programs' enforcement of their guidelines).

[336] *See, e.g.,* CARU, at 11; SuperAwesome, at 31; CIPL, at 7.

[337] TRUSTe, at 3.

[338] CARU, at 11.

[339] SuperAwesome, at 31.

[340] *See* Part IV.F.

[341] SuperAwesome, at 31.

[342] CIPL, at 7.

[343] This requirement will additionally allow the Commission to monitor whether subject operators are switching FTC-approved COPPA Safe Harbor programs for forum shopping purposes as one commenter noted. *See* Representative Kathy Castor, at 2. This concern was also raised during the COPPA Workshop, in which an employee of an FTC-approved COPPA Safe Harbor program noted that ''one of the issues that we have with safe harbor right now is the shopping around . . . we've lost a few, actually, where we've refused to allow standards that we don't think are meeting the requirements of COPPA and our program and they've gone elsewhere.'' *See* C. Quinn, Remarks from the *State of the World in Children's Privacy Panel* at *The Future of the COPPA Rule: An FTC Workshop* 37–38 (Oct. 7, 2019), *available at https://www.ftc.gov/system/files/documents/public_events/1535372/transcript_of_coppa_workshop_part_1_1.pdf.*

subject operator). These proposed changes will enhance the Commission's ability to oversee FTC-approved COPPA Safe Harbor programs.

Additionally, one FTC-approved COPPA Safe Harbor program recommended that the Commission consider conducting audits of each FTC-approved COPPA Safe Harbor program and publishing an audit checklist after completing each audit.[344] Relatedly, another commenter suggested that the Rule should require FTC-approved COPPA Safe Harbor programs to demonstrate on a periodic basis that they are regularly assessing and updating their programs to comply with COPPA.[345]

The Commission agrees that, in addition to its current oversight of FTC-approved COPPA Safe Harbor programs, including review of the FTC-approved COPPA Safe Harbor programs' annual reports discussed in this part of the preamble, regular audits of FTC-approved COPPA Safe Harbor programs' technological capabilities and mechanisms for assessing subject operators' fitness for maintaining membership could further strengthen oversight. To that end, the Commission proposes to add a new § 312.11(f) requiring FTC-approved COPPA Safe Harbor programs to submit triennial reports that provide details about those issues.[346]

In terms of transparency, several commenters recommended that the Commission require programs to publish lists of their certified members.[347] One FTC-approved COPPA Safe Harbor program, however, posited that public disclosure of membership lists would lead to the ''poaching'' of safe harbor members and recommended that the Rule require safe harbors instead to provide service-level certification information to the FTC confidentially.[348] Another disagreed that public disclosure of membership lists would lead to the stealing of members, stating that it has always publicly disclosed the products it has certified.[349] A coalition of consumer groups supported greater transparency and argued that FTC-approved COPPA Safe Harbor programs' current practices with respect to whether and where subject operators display membership seals makes it difficult for parents and others to determine whether websites or online services are participants of an FTC-approved COPPA Safe Harbor program.[350]

The Commission proposes requiring that FTC-approved COPPA Safe Harbor programs publish lists of their subject operators. While the Commission understands certain commenters' concerns that the publication of such a list could result in the loss of subject operators to other FTC-approved COPPA Safe Harbor programs, the Commission believes that such concerns are outweighed by the benefits created by increasing transparency around FTC-approved COPPA Safe Harbor programs. Therefore, the Commission proposes adding this requirement as new paragraph § 312.11(d)(4).

3. Revocation of Approval of Self-Regulatory Program Guidelines (Current § 312.11(f), Proposed To Be Renumbered as § 312.11(g))

Current § 312.11(f), which the Commission proposes to renumber as § 312.11(g) in light of the new proposed § 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. In addition, current § 312.11(f) requires FTC-approved COPPA Safe Harbor programs that the Commission had approved before the Commission amended the Rule in 2013 to submit by March 1, 2013 proposed modifications to bring their guidelines into compliance with the 2013 Rule amendments.

Because the March 1, 2013 deadline has passed and is no longer relevant, the Commission proposes to strike from renumbered § 312.11(g) the requirement that FTC-approved COPPA Safe Harbor programs submit proposed modifications to their guidelines. If the Commission proceeds to modify the Rule as discussed in this notice, the Commission will provide an appropriate deadline for safe harbor programs to submit proposed modifications to bring their guidelines into compliance with such amendments.

I. Voluntary Commission Approval Processes (16 CFR 312.12)

The Commission also proposes making a few technical 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.'' [351]

V. Request for Comment

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before March 11, 2024. Write ''COPPA Rule Review, Project No. P195404'' on your comment. Your comment—including your name and your State—will be placed on the public record of this proceeding, including the *https://www.regulations.gov* website.

Postal mail addressed to the Commission is subject to delay due to heightened security screening. As a result, we encourage you to submit your comments online. To make sure that the Commission considers your online comment, you must file it at *https://www.regulations.gov,* by following the instructions on the web-based form.

If you file your comment on paper, write ''COPPA Rule Review, Project No. P195404'' on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC–5610 (Annex E), Washington, DC 20580. If possible, please submit your paper comment to the Commission by overnight service.

Because your comment will be placed on the publicly accessible website at *https://www.regulations.gov,* you are solely responsible for making sure that your comment does not include any sensitive or confidential information. In particular, your comment should not include any sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other State identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure that your comment does not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any ''trade secret or any commercial or financial information which . . . is privileged or confidential''—as provided by section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2)—including in particular competitively sensitive information such as costs,

[344] ESRB, at 5. This commenter suggested biennial audits, however on balance, the Commission believes that conducting such reviews every three years is appropriate.

[345] CIPL, at 7.

[346] Because the Commission proposes to add a new § 312.11(f), the Commission also proposes to renumber existing §§ 312.11(f) and 312.11(g) as 312.11(g) and 312.11(h), respectively.

[347] SuperAwesome, at 31; S. Egelman, at 5; kidSAFE, at 17.

[348] ESRB, at 5 (also asserting that there is a lack of evidence showing that consumers want access to such lists).

[349] kidSAFE, at 17.

[350] Joint Consumer Groups, at 19–20.

[351] 15 U.S.C. 6501(4).

sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled ''Confidential,'' and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted publicly at *https://www.regulations.gov*—as legally required by FTC Rule 4.9(b)—we cannot redact or remove your comment, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

Visit the FTC website to read this publication and the news release describing it, and visit *https://www.regulations.gov/docket/FTC-2023-0076* to read a plain-language summary of the proposed Rule. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before March 11, 2024. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see *https://www.ftc.gov/site-information/privacy-policy*.

VI. 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.[352] 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.'' [353] 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 March 31, 2025 (OMB Control No. 3084–0117).

The proposed amendments to the COPPA Rule would 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. The proposed Rule would also increase disclosure obligations for operators and FTC-approved COPPA Safe Harbor programs, and FTC-approved COPPA Safe Harbor programs would also face additional reporting obligations under the proposed Rule. Commission staff does not believe that the proposed Rule would increase operators' recordkeeping obligations.

The Commission invites comments on: (1) whether the proposed collection of information is necessary for the proper performance of the functions of the FTC, including whether the information will have practical utility; (2) the accuracy of the FTC's estimate of the burden of the proposed collection of information; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of collecting information on those who respond. Written comments and recommendations for the proposed information collection should also be sent within 30 days of publication of this document to *https://www.reginfo.gov/public/do/PRAMain.* Find this particular information collection by selecting ''Currently under Review—Open for Public Comments'' or by using the search function. The *reginfo.gov* web link is a United States Government website produced by OMB and the General Services Administration. Under PRA requirements, OMB's Office of Information and Regulatory Affairs reviews federal information collections.

Estimated Additional Annual Hours Burden

A. Number of Respondents

As noted in the Regulatory Flexibility section of this NPRM, Commission staff estimates that there are currently approximately 5,710 operators subject to the Rule. Commission staff believes that the changes that are most likely to affect the number of operators subject to the Rule are the Commission's proposed changes to the Rule's definition of ''website or online service directed to children.'' Of most relevance to this discussion, the Commission proposes to modify paragraph 2 of this definition to account for third parties with actual knowledge that they collect children's information from users of a child-directed site or service, even if such third parties do not collect the information *directly* from such users. While Commission staff contemplates that this modification could increase the number of operators subject to the Rule's requirements, staff does not have sufficient evidence to estimate the amount of increase, and therefore the Commission welcomes comment on this issue. Commission staff does not expect that the other proposed modifications to this definition, such as the additional exemplar factors the Commission will consider in determining whether a site or service is child-directed, will alter the number of operators subject to the Rule.

Commission staff does not believe that other proposed modifications to the Rule's definitions will affect the number of operators subject to the Rule. For example, Commission staff does not expect that the Commission's proposed addition of ''biometric identifiers'' to the Rule's definition of ''personal information'' will significantly alter the number of operators subject to the Rule. Commission 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 proposed revisions to the Rule's definitions might result in minor additional numbers of operators being subject to the Rule, Commission 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, Commission staff retains its recently published estimate of 280 new operators per year.[354] Commission staff also retains its estimate that no more than one additional FTC-approved COPPA Safe Harbor program applicant is likely to submit a request within the next three years of PRA clearance.

B. Recordkeeping Hours

While the proposed 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 proposed Rule, each operator's security

[352] 44 U.S.C. 3502(3)(A)(i).

[353] *See* 44 U.S.C. 3502(3)(A).

[354] *See* 2022 COPPA PRA Supporting Statement, available at *https://omb.report/icr/202112-3084-002/doc/119087900* (hereinafter, ''2022 COPPA PRA Supporting Statement'').

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. Similarly, the instituted data retention policy will differ depending on the operator's business practices. Thus, although each operator must summarize its compliance efforts in one or more written documents, the discretionary balancing of factors and circumstances that the proposed Rule allows does not require entities to answer ''identical questions'' and therefore does not trigger the PRA's requirements.

Separately, the proposed Rule imposes minimal recordkeeping requirements for FTC-approved COPPA Safe Harbor programs. However, FTC staff understands that most of the records listed in the COPPA Rule's safe harbor recordkeeping provisions consist of documentation that covered entities retain in the ordinary course of business irrespective of the COPPA Rule. OMB excludes from the definition of PRA burden, among other things, recordkeeping requirements that customarily would be undertaken independently in the normal course of business.[355] In staff's view, any incremental burden posed by the proposed Rule—such as that to include additional content in annual reports, submit a report to the Commission every three years detailing technological capabilities and mechanisms, and publicly post membership lists—would be marginal.

C. Disclosure Hours

1. New Operators' Disclosure Burden

FTC staff estimates that the Rule affects approximately 280 new operators per year.[356] 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, the direct notice to parents.[357] In addition, the proposed Rule includes a new requirement that operators establish, implement, maintain, and disclose a data retention policy. Staff estimates it will require, on average, approximately 10 hours to meet the data retention policy requirement. In combining these figures, Commission staff estimates that these disclosure requirements will require 70 hours of burden per operator. This yields an estimated annual hours burden of 19,600 hours (280 respondents × 70 hours).

2. Existing Operators' Disclosure Burden

The proposed Rule imposes various new disclosure requirements on operators. Specifically, the proposed amendments require operators to update existing disclosures, namely to update the direct and online notices with additional information about the operators' information practices. Additionally, some operators may have to provide disclosures that were not previously required under the Rule. For operators utilizing the support for the internal operations exception, 16 CFR 312.5(c)(7), the proposed Rule will now require such operators to provide an online notice. Similarly, the proposed Rule will require operators utilizing the proposed school authorization exception, which is newly numbered as 16 CFR 312.5(c)(10), to provide an online notice, a direct notice to the school, and enter into a written agreement with the school. Additionally, the proposed Rule requires operators to disclose a data retention policy.

Commission staff believes that an existing operator's time to make these changes to its online and direct notices 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. Regarding the written agreement, FTC staff understands that many ed tech operators enter into standard contracts with schools, school districts, and other education organizations across the country, and this requirement is not intended to interfere with such contractual arrangements. Therefore, this agreement likely consists of documentation that covered entities retain in the ordinary course of business irrespective of the COPPA Rule. As noted above, OMB excludes from the definition of PRA burden, among other things, recordkeeping requirements that customarily would be undertaken independently in the normal course of business.[358] Additionally, as discussed previously, Commission 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 approximately 70 hours of burden. Annualized over three years of PRA clearance, this amounts to approximately 23 hours (70 hours ÷ 3 years) per operator each year. Aggregated for the 5,710 existing operators, the annualized disclosure burden for these requirements would be approximately 131,330 hours per year (5,710 respondents × 23 hours).

The proposed Rule will also require each FTC-approved COPPA Safe Harbor program to provide a list of all current subject operators on each of the FTC-approved COPPA Safe Harbor program's websites and online services, and the proposed Rule further requires that such list be updated every six months thereafter. Because FTC-approved COPPA Safe Harbor programs likely already keep up-to-date lists of their subject operators, Commission 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, Commission 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).

D. Reporting Hours

The proposed amendments will require FTC-approved COPPA Safe Harbor programs to include additional content in their annual reports. The proposed 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. Commission 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 (300 hours) FTC-approved COPPA Safe Harbor programs, this amounts to an estimated cumulative reporting burden of 350 hours per year (7 respondents × 50 hours).

Regarding the reports that the proposed Rule will require FTC-approved Safe Harbor programs to

[355] *See* 5 CFR 1320.3(b)(2).

[356] This consists of certain traditional website operators, mobile app developers, plug-in developers, and advertising networks.

[357] *See, e.g.,* Children's Online Privacy Protection Rule, Notice, 86 FR 55609 (Oct. 6, 2021), available at *https://www.govinfo.gov/content/pkg/FR-2021-10-06/pdf/2021-21753.pdf;* 2022 COPPA PRA Supporting Statement.

[358] *See* 5 CFR 1320.3(b)(2).

submit to the Commission every three years, § 312.11(c)(1) of the Rule already requires FTC-approved COPPA Safe Harbor programs to include similar information in their initial application to the Commission. Specifically, § 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. Staff estimates that reviewing and updating existing information to comply with proposed § 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 up to 4 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, FTC staff anticipates that no more than one additional FTC-approved COPPA Safe Harbor program applicant is likely to submit a request 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 28 hours per year (7 respondents × 4 hours).

E. Labor Costs

1. Disclosure

a. New Operators

As previously noted, Commission staff estimates a total annual burden of 19,600 hours (280 respondents × 70 hours). Consistent with its past estimates and based on its 2013 rulemaking record,[359] 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, Commission staff estimates that approximately 16,333 of the estimated 19,600 hours required will be completed by legal staff.

Regarding legal personnel, Commission 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. Assuming two-thirds of such work is done by junior associates at a rate of approximately $300 per hour, and one-third by senior partners at approximately $600 per hour, the weighted average of outside counsel costs would be approximately $400 per hour.[360]

FTC staff anticipates that computer programmers responsible for posting privacy policies and implementing direct notices and parental consent mechanisms would account for the remaining approximately 3,267 hours. FTC staff estimates an hourly wage of $57 (rounded to the nearest dollar) for technical assistance, based on Bureau of Labor Statistics (''BLS'') data.[361] Accordingly, associated annual labor costs would be $6,719,419 [(16,333 hours × $400/hour) + (3,267 hours × $57/hour)] for the estimated 280 new operators.

b. Existing Operators

As previously discussed, Commission staff estimates that the annualized disclosure burden for these requirements for the 5,710 existing operators would be 131,330 hours per year. Thus, apportioned five to one, this amounts to 109,442 hours of legal and 21,888 hours of technical assistance. Applying hourly rates of $400 and $57, respectively, for these personnel categories, associated labor costs would total approximately $45,024,416 ($43,776,800 + $1,247,616).

As noted, Commission staff estimates a cumulative disclosure burden of 10 hours per year for FTC-approved COPPA Safe Harbor programs. 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 70 hours per year (7 respondents × 10 hours).

Industry sources have advised that the labor to comply with requirements from FTC-approved COPPA Safe Harbor programs would be attributable to the efforts of in-house lawyers. To determine in-house legal costs, FTC staff applied an approximate average between the BLS reported mean hourly wage for lawyers ($78.74),[362] and estimated in-house hourly attorney rates ($300) that are likely to reflect the costs associated with the proposed Rule's safe harbor requirements. This yields an approximate hourly rate of $190. Applying this hourly labor cost estimate to the hours burden associated with the cumulative disclosure burden for FTC-approved COPPA Safe Harbor programs yields an estimated annual burden of $13,300 (70 hours × $190).

2. Reporting

As previously noted, Commission staff estimates an estimated cumulative reporting burden of 378 hours per year for FTC-approved COPPA Safe Harbor programs. The approximate hourly rate for labor to comply with requirements from FTC-approved COPPA Safe Harbor programs is $190, as previously calculated. Applying this hourly labor cost estimate to the hours burden associated with the cumulative reporting burden for FTC-approved COPPA Safe Harbor programs yields an estimated annual labor cost burden of $71,820 (378 hours × $190).

F. 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 Rule's notice requirements, the proposed Rule should not impose any additional capital or other non-labor costs.

VII. Regulatory Flexibility Act

The Regulatory Flexibility Act (''RFA''), as amended by the Small Business Regulatory Enforcement Fairness Act of 1996, requires an agency to either provide an Initial Regulatory

[359] *See, e.g.,* 78 FR 3972 at 4007; 2022 COPPA PRA Supporting Statement.

[360] These estimates are drawn from the ''Laffey Matrix.'' The Laffey Matrix is a fee schedule used by many United States courts for determining the reasonable hourly rates in the District of Columbia for attorneys' fee awards under federal fee-shifting statutes. It is used here as a proxy for market rates for litigation counsel in the Washington, DC area. For 2020–2021, rates in the table range from $333 per hour for most junior associates to $665 per hour for the most senior partners. *See* Laffey Matrix, Civil Division of the United States Attorney's Office for the District of Columbia, United States Attorney's Office, District of Columbia, Laffey Matrix B 2015–2021, *available at https://www.justice.gov/usao-dc/page/file/1305941/download.*

[361] The estimated mean hourly wage for technical labor support ($57) is based on an average of the mean hourly wage for computer programmers, software developers, and information security analysts as reported by the Bureau of Labor Statistics. *See Occupational Employment and Wages—May 2022,* Table 1 (National employment and wage data from the Occupational Employment and Wage Statistics survey by occupation, May 2022), *available at https://www.bls.gov/news.release/ocwage.t01.htm* (hereinafter, ''BLS Table 1'').

[362] *See* BLS Table 1 (lawyers).

Flexibility Analysis (''IRFA'') with a proposed rule, or certify that the proposed Rule will not have a significant impact on a substantial number of small entities.[363]

The Commission does not expect that the proposed Rule, if adopted, would have a significant impact on a substantial number of small entities. Among other things, as discussed further below, many of the proposed amendments reflect modest changes to the Rule, including to clarify definitions, increase content requirements for existing notices, increase specificity for existing security requirements, increase clarity on existing retention and deletion requirements, and increase specificity on certain reporting requirements. While the proposed amendments may 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 does not anticipate this will require significant additional costs to entities covered by the Rule. Instead, some of the proposed amendments, such as amendments to create exceptions for the Rule's verifiable parental consent requirements, may even reduce costs for many entities covered by the Rule.

Although the Commission certifies under the RFA that the proposed 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, the Commission has determined that it is appropriate to publish an IRFA in order to inquire into the impact of the proposed Rule on small entities. The Commission invites comment on the burden on any small entities that would be covered and has prepared the following analysis.

A. Reasons for the Proposed Rule

As discussed in Part I, the Commission commenced a review of the COPPA Rule on July 25, 2019, noting that questions had arisen about the Rule's application to the ed tech sector, voice-enabled connected devices, and general audience platforms that host third-party child-directed content. After review of the comments received, the Commission concludes that there is a need to update certain Rule provisions to account for changes in technology and online practices, and where appropriate, to clarify and streamline the Rule. Accordingly, the Commission proposes modifications to the Rule in the following areas: Scope of Regulations; Definitions; Notice; Parental Consent; Parental Right to Review; Confidentiality and Security of Children's Personal Information; Data Retention and Deletion; Safe Harbor Programs; and Voluntary Commission Approval Processes.

B. Statement of Objectives and Legal Basis

The objectives of the Proposed Rule are to update the 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 proposed Rule is the Children's Online Privacy Protection Act, 15 U.S.C. 6501 *et seq.*

C. Description and Estimated 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 website or online service with actual knowledge that it is collecting personal information from children. The Rule also applies to operators of websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children.

The Commission staff is unaware of any empirical evidence concerning the number of operators subject to the Rule. However, based on the previous estimates [364] and the Commission's compliance monitoring efforts in the areas of children's privacy, Commission staff estimates that approximately 5,710 operators may be subject to the Rule's requirements, with approximately 280 new operators per year.

Under the Small Business Size Standards issued by the Small Business Administration, ''web search portals and all other information services'' qualify as small businesses if they have 1,000 or fewer employees.[365] Commission staff estimates that approximately 80% of operators potentially subject to the Rule qualify as small entities. The Commission staff bases this estimate on its experience in this area, which includes its law enforcement activities, oversight of FTC-approved COPPA Safe Harbor programs, conducting relevant workshops, and discussions with industry and privacy professionals. The Commission seeks comment and information with regard to the estimated number or nature of small business entities on which the proposed Rule would have a significant economic impact.

D. Projected Reporting, Recordkeeping, and Other Compliance Requirements

The proposed amended Rule would impose reporting, recordkeeping, and other compliance requirements within the meaning of the PRA, as set forth in Part VI of this NPRM. Therefore, the Commission is submitting the proposed requirements to OMB for review before issuing a final rule.

For example, while not constituting a ''collection of information'' under the PRA, the proposed Rule would require operators to establish, implement, and maintain a written comprehensive security program. The proposed Rule would also likely increase the disclosure requirements for covered operators, and it would likely increase the disclosure and reporting requirements for FTC-approved COPPA Safe Harbor programs. Specifically, the proposed 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 were not previously required under the Rule. Additionally, the proposed Rule requires operators to disclose a data retention policy.

The proposed Rule will also require each FTC-approved COPPA Safe Harbor program to provide a list of all current subject operators on each of the FTC-approved COPPA Safe Harbor program's websites and online services, and the proposed Rule further requires that such list be updated every six months thereafter. The proposed 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 proposed amendments is discussed in the PRA section of this document, and there should be no

[363] 5 U.S.C. 603–605.

[364] *See, e.g.,* 78 FR 3972 at 4000.

[365] *See* U.S. Small Business Administration Table of Small Business Size Standards Matched to North American Industry Classification System Codes, available at *https://www.sba.gov/sites/sbagov/files/2023-03/Table%20of%20Size%20Standards_Effective%20March%2017%2C%202023%20%281%29%20%281%29_0.pdf.*

difference in that burden as applied to small businesses. 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 proposed 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, Commission staff estimates that there are approximately 5,710 websites or online services that qualify as operators under the proposed Rule, and that approximately 80% of such operators qualify as small entities under the SBA's Small Business Size standards. The Commission invites comment and information on these issues.

E. Identification of Duplicative, Overlapping, or Conflicting Federal Rules

The Commission has not identified any other federal statutes, rules, or policies that would duplicate, overlap, or conflict with the proposed Rule. While the proposed Rule includes amendments related to schools, the Commission believes it has drafted the proposed Rule to ensure it does not duplicate, overlap, or conflict with the Family Educational Rights and Privacy Act. The Commission invites comment and information on this issue.

F. Discussion of Significant Alternatives

In drafting the proposed Rule, the Commission has made every effort to avoid unduly burdensome requirements for entities. The Commission believes that the proposed amendments are necessary to continue to protect children's online privacy in accordance with the purposes of COPPA. For each of the proposed amendments, the Commission has attempted to tailor the provision to any concerns evidenced by the record to date. On balance, the Commission believes that the benefits to children and their parents outweigh any potential increased costs of implementation to industry.

For example, some commenters called for the Commission to implement specific time limits on data retention, noting that operators could read the Rule as currently written to allow indefinite retention of personal information. Rather than impose specific limitations that would apply to operators that collect different types of personal information for varying types of activities, the Commission alternatively proposes to require operators to establish a written data retention policy that sets forth a timeframe for deletion and explicitly prohibits indefinite retention.

Additionally, the Commission has taken care in developing the proposed amendments to set performance standards that will establish the objective results that must be achieved by regulated entities, but do not mandate a particular technology that must be employed in achieving these objectives. For example, the proposed Rule does not mandate the technology that must be used to establish, implement, and maintain the children's written information security program and related safeguards required under newly-numbered § 312.8(b).

The Commission seeks comments on ways in which the proposed Rule could be modified to reduce any costs or benefits for small entities.

VIII. Communications by Outside Parties to the Commissioners or Their Advisors

Written communications and summaries or transcripts of oral communications respecting the merits of this proceeding, from any outside party to any Commissioner or Commissioner's advisor, will be placed on the public record. *See* 16 CFR 1.26(b)(5).

IX. Questions for the Proposed Revisions to the Rule

The Commission is seeking comment on various aspects of the proposed Rule and is particularly interested in receiving comment on the questions that follow. These questions are designed to assist the public and should not be construed as a limitation on the issues on which public comment may be submitted. Responses to these questions should cite the numbers and subsections of the questions being answered. For all comments submitted, please submit any relevant data, statistics, or any other evidence, upon which those comments are based.

General Question

1. Please provide comment on any or all of the provisions in the proposed Rule. For each provision commented on, please describe: (1) the impact of the provision(s) (including any benefits and costs), if any; and (2) what alternatives, if any, the Commission should consider, as well as the costs and benefits of those alternatives.

Definitions

2. As part of the Rule review that led to the 2013 Amendments, the Commission determined that an operator will not be deemed to have ''collected'' (as that term is defined in the Rule) personal information from a child when it employs technologies reasonably designed to delete all or virtually all personal information input by children before making information publicly available.[366] The Commission is concerned that, if automatic moderation or filtering technologies can be circumvented, reliance on such technologies may not be appropriate in a context where a child is communicating one to one with another person privately, as opposed to posting information online publicly. Should the Commission retain its position that an operator will not be deemed to have ''collected'' personal information, and therefore does not have to comply with the Rule's requirements, if it employs automated means to delete all or virtually all personal information from one-to-one communications?

3. The Commission proposes to include mobile telephone numbers within the definition of ''online contact information'' so long as such information is used only to send text messages. This proposed modification would permit operators to send text messages to parents to initiate obtaining verifiable parental consent. Does allowing operators to contact parents through a text message to obtain verifiable parental consent present security risks to the recipient of the text message, particularly if the parent would need to click on a link provided in the text message?

4. In conjunction with the 2013 Amendments, the Commission acknowledged that screen and user names have increasingly become portable across multiple websites or online services, and that such identifiers permit the direct contact of a specific individual online.[367] Through the 2013 Amendments, the Commission defined personal information to include screen or user names only to the extent these

[366] 76 FR 59804 at 59808.

[367] 76 FR 59804 at 59810.

identifiers function in the same way as ''online contact information'' as the Rule defines that term. Since 2013, the use of screen and user names has proliferated across websites and online services, including on online gaming platforms that allow users to directly engage with each other. The Commission is concerned that children may use the same screen or user name on different sites and services, potentially allowing other users to contact and engage in direct communications with children on another online service.

a. Should screen or user names be treated as online contact information, even if the screen or user name does not allow one user to contact another user through the operator's website or online service, when the screen or user name 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 website or online service that does allow such contact?

b. Are there measures an operator can take to ensure that a screen or user name cannot be used to permit the direct contact of a person online?

5. The Commission proposes adding biometric identifiers such as fingerprints, retina and iris patterns, a DNA sequence, and data derived from voice data, gait data, or facial data to the definition of ''personal information.'' Should the Commission consider including any additional biometric identifier examples to this definition? Are there exceptions to the Rule's requirements that the Commission should consider applying to biometric data, such as exceptions for biometric data that has been promptly deleted?

6. The use of avatars generated from a child's image has become popular in online services, such as video games. Should an avatar generated from a child's image constitute ''personal information'' under the COPPA Rule even if the photograph of the child is not itself uploaded to the site or service and no other personal information is collected from the child? If so, are these avatars sufficiently covered under the current COPPA Rule, or are further modifications to the definition required to cover avatars generated from a child's image?

7. The definition of ''personal information'' includes a Social Security number. Should the Commission revise this definition to list other government-issued identifiers specifically? If so, what type of identifiers should be included?

8. The definition of ''personal information'' includes ''information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in [the Rule's definition of 'personal information'].'' Does the phrase ''concerning the child or parents of that child'' require further clarification?

9. Certain commenters recommended modifications to the ''support for the internal operations of the website or online service'' definition, including to limit personalization to ''user-driven'' actions and to exclude methods designed to maximize user engagement. Under what circumstances would personalization be considered ''user-driven'' versus personalization driven by an operator? How do operators use persistent identifiers, as defined by the COPPA Rule, to maximize user engagement with a website or online service?

10. Operators can collect persistent identifiers for contextual advertising purposes without parental consent so long as they do not also collect other personal information. Given the sophistication of contextual advertising today, including that personal information collected from users may be used to enable companies to target even contextual advertising to some extent, should the Commission consider changes to the Rule's treatment of contextual advertising?

11. With regard to the definition of ''website or online service directed to children,'' the Commission would like to obtain additional comment on whether it should provide an exemption for operators from being deemed a child-directed website or online service if such operators undertake an analysis of their audience composition and determine no more than a specific percentage of its users are likely to be children under 13.

a. Should the COPPA Rule offer an exemption or other incentive to encourage operators to conduct an analysis of their user bases?

b. If the COPPA Rule should include such an exemption or other incentive, what are the reliable means by which operators can determine the likely ages of their sites' or services' users?

c. As part of this exemption or incentive, should the COPPA Rule identify which means operators must utilize to determine the likely ages of their users? If so, how should the COPPA Rule identify such means?

d. If the COPPA Rule should include such an exemption or other incentive, what should be the appropriate percentage of users to qualify for this exemption or incentive?

e. Would such an exemption be inconsistent with the COPPA Rule's multi-factor test for determining whether a website or online service, or a portion thereof, is directed to children?

Notice

12. The Commission proposes requiring operators that share personal information with third parties to identify those third parties or specific categories of those third parties in the direct notice to the parent. Is this information better positioned in the direct notice required under § 312.4(c), or should it be placed in the online notice required under § 312.4(d)?

Parental Consent

13. Can platforms play a role in establishing consent mechanisms to enable app developers or other websites or online services to obtain verifiable parental consent? If so, what benefits would a platform-based common consent mechanism offer operators and parents? What steps can the Commission take to encourage the development of platform-based consent mechanisms?

14. To effectuate § 312.5(a)(2), which requires operators to give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of the child's personal information to third parties, the Commission proposes requiring operators to obtain separate verifiable parental consent prior to disclosing a child's personal information, unless such disclosure is integral to the nature of the website or online service. Should the Commission implement such a requirement? Should the consent mechanism for disclosure be offered at a different time and/or place than the mechanism for the underlying collection and use? Is the exception for disclosures that are integral to the nature of the website or online service clear, or should the Commission clarify which disclosures are integral? Should the Rule require operators to state which disclosures are integral to the nature of website or online service?

15. As noted in Part IV.C.3.c., the Commission proposes to modify § 312.5(c)(4) to prohibit operators from utilizing this exception to encourage or prompt use of a website or online service. Are there other engagement techniques the Rule should address? If so, what section of the Rule should address them? What types of personal information do operators use when utilizing engagement techniques? Additionally, should the Rule differentiate between techniques used solely to promote a child's engagement

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

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

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

17. COPPA and § 312.7 of the Rule prohibit operators from conditioning a child's participation in an activity on disclosing more personal information than is reasonably necessary to participate in such activity.

a. What efforts are operators taking to comply with § 312.7? Are these efforts taken on a website-wide or online service-wide basis, or are operators imposing efforts on a more granular level?

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

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

18. The Commission is considering adding new language to address the meaning of ''activity,'' as that term is used in § 312.7. Specifically, the Commission is considering including language in § 312.7 to provide that an ''activity'' means ''any activity offered by a website or online service, whether that activity is a subset or component of the website or online service or is the entirety of the website or online service.'' Should the Commission make this modification to the Rule? Is this modification necessary in light of the breadth of the plain meaning of the term ''activity''?

Safe Harbor

19. What types of conflicts would affect an FTC-approved COPPA Safe Harbor program from effectively assessing a subject operator's fitness for membership in the FTC-approved COPPA Safe Harbor program? What policies do FTC-approved COPPA Safe Harbor programs have in place to prevent such conflicts?

Effective Date

20. As part of the issuance of the initial Rule and the 2013 Amendments, the Commission stated that the Rule and amended Rule, respectively, would become effective approximately six months after issuance of the Commission's final rule in the **Federal Register**. The Commission requests comment on whether such timeframe is appropriate for the modifications set forth during this Rule review that do not specify an effective date.

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 proposes to amend 16 CFR 312 as follows:

PART 312—CHILDREN'S ONLINE PRIVACY PROTECTION RULE

■ 1. The authority for part 312 continues to read:

Authority: 15 U.S.C. 6501 through 6508.

■ 2. Revise § 312.1 to read as follows:

§ 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.

■ 3. In § 312.2:

■ a. Revise the definition of *Disclose or disclosure;*

■ b. Add in alphabetical order a definition for *Mixed audience website or online service;*

■ c. Revise the definition of *Online contact information;*

■ d. Revise the introductory text and paragraph (2) of the definition of *Operator;*

■ e. Republish the introductory text, revise paragraphs (7) and (9), redesignate paragraph (10) as paragraph (11), and add a new paragraph (10) to the definition of *Personal information;*

■ f. Add in alphabetical order definitions for *School* and *School-authorized education purpose;*

■ g. Remove the words ''Web Site'' and add in their place the word ''Web site'' in the term *Support for the internal operations of the website or online service* and in the definition, republish paragraph (1) introductory text and revise paragraphs (1)(i), (iii), (iv), (v), and (vii) and (2);

■ h. Revise the definition of *Third party; and*

■ i. Remove the definition of *Web site or online service directed to children* and add inits place in alphabetical order a definition for *Website or online service directed to children.*

The additions, republications, and revisions read as follows:

§ 312.2 Definitions.

* * * * *

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.

* * * * *

Mixed audience website or online service means a website or online service that is directed to children under the criteria set forth in paragraph (1) of the definition of website or online service directed to children, but that does not target children as its primary audience, and does not collect personal information from any visitor prior to collecting age information or using another means that is reasonably calculated, in light of available technology, to determine whether the visitor is a child. Any collection of age information, or other means of determining whether a visitor is a child, must be done in a neutral manner that does not default to a set age or encourage visitors to falsify age information.

* * * * *

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 an identifier such as a mobile telephone number provided the operator uses it only to send a text message.

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 one 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:

* * * * *

(2) The operator benefits by allowing another person to collect personal information directly from users of such website or online service.

* * * * *

Personal information means individually identifiable information about an individual collected online, including:

* * * * *

(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;

* * * * *

(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, including fingerprints or handprints; retina and iris patterns; genetic data, including a DNA sequence; or data derived from voice data, gait data, or facial data; 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.

* * * * *

School means a State educational agency or local educational agency as defined under Federal law, as well as an institutional day or residential school, including a public school, charter school, or private school, that provides elementary or secondary education, as determined under State law.

School-authorized education purpose means any school-authorized use related to a child's education. Such use shall be limited to operating the specific educational service that the school has authorized, including maintaining, developing, supporting, improving, or diagnosing the service, provided such uses are directly related to the service the school authorized. School-authorized education purpose does not include commercial purposes unrelated to a child's education, such as advertising.

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;

* * * * *

(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;

* * * * *

(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) through(vii) of this definition, the information collected for the activities listed in paragraphs (1)(i) through (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, in connection with processes that encourage or prompt use of a website or online service, 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 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.

■ 4. Revise § 312.3 introductory text and paragraph (a) to read as follows:

§ 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));

* * * * *

■ 5. In § 312.4:

■ a. Revise paragraphs (b), (c) introductory text, (c)(1), (c)(2) introductory text, and (c)(2)(i) and (iii);

■ b. Add paragraph (c)(5);

■ c. Revise paragraph (d); and

■ d. Add paragraph (e);

The revisions and additions read as follows:

§ 312.4 Notice.

* * * * *

(b) *Direct notice to the parent or school.* An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child or, if applicable, the child's school 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 or the school has previously authorized.

(c) *Content of the direct notice*—(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 nature of 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;

* * * * *

(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

* * * * *

(5) *Content of the direct notice to the school under § 312.5(c)(10) (Notice to a School for Educational Services).* This direct notice shall set forth:

(i) That a school's authorization 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 school does not provide such authorization;

(ii) That the operator's use and disclosure of personal information collected from the child is limited to a school-authorized education purpose;

(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 school provide authorization;

(iv) Where the operator discloses the personal information to third parties, the identities or specific categories of such third parties and the specific school-authorized education purposes for such disclosure, should the school provide authorization;

(v) A hyperlink to the operator's online notice of its information practices required under paragraphs (d) and (e) of this section; and

(vi) The means by which the school can authorize the collection, use, and disclosure of the information.

(d) *Notice on the website or online service.* In addition to the direct notice, 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 or specific categories of any third parties to which the operator discloses personal information and the purposes for such disclosures; and the operator's data retention policy as required under § 312.10;

(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, 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);

(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.

(e) *Additional notice on the website or online service where an operator has collected personal information under § 312.5(c)(10).* In addition to the applicable requirements in paragraph (d) of this section, where an operator has collected personal information under § 312.5(c)(10), an operator's online notice of its information practices with regard to children must state that the operator has obtained authorization from a school to collect a child's personal information; that the operator will use and disclose the information for a school-authorized education purpose and no other purpose; that the school may review the information; and that the school may request deletion of the child's personal information, and the procedures for doing so.

■ 6. In § 312.5:

■ a. Revise paragraph (a)(2) and paragraph (b)(2)(ii);

■ b. Redesignate paragraph (b)(2)(vi) as (b)(2)(viii);

■ c. Republish newly designated paragraphs (b)(2)(viii);

■ d. Add new paragraphs (b)(2)(vi) and (vii);

■ e. Revise paragraphs (c)(2) and (4), (c)(6)(i) and (iv), (c)(7) and (8); and

■ f. Add paragraphs (c)(9) and (10);

The revisions, republication, and additions read as follows:

§ 312.5 Parental consent.

(a) * * *

(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 nature of the website or online service. An operator required to give the parent this option must obtain separate verifiable parental consent to such disclosure, and the operator may not condition access to the website or online service on such consent.

(b) * * *

(2) * * *

(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;

* * * * *

(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 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.

* * * * *

(c) * * *

(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);

* * * * *

(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. Provided, however, that an operator may not utilize this exception to encourage or prompt use of a website or online service. An operator utilizing this exception for permissible purposes 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;

* * * * *

(6) * * *

(i) Protect the security or integrity of the website or online service;

* * * * *

(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;

(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); or

(10) Where the operator obtains school authorization for the collection of the child's personal information for a school-authorized education purpose. In such a case, the operator must ensure that the school receives notice as described in § 312.4(c)(5) and must have a written agreement with the school that:

(i) Indicates the name and title of the person providing authorization and attests that the person has the authority to do so;

(ii) Limits the operator's use and disclosure of the personal information to a school-authorized education purpose only and no other purpose;

(iii) Provides that the operator is under the school's direct control with regard to the use, disclosure, and maintenance of the personal information collected from the child pursuant to school authorization; and

(iv) Sets forth the operator's data retention policy with respect to such information in accordance with § 312.10.

■ 7. In § 312.6:

■ a. Revise the section heading and paragraph (a) introductory text;

■ b. Redesignate paragraphs (b) and (c) as paragraphs (c) and (d);

■ c. Add new paragraph (b); and

■ d. Republish newly redesignated paragraphs (c) and (d).

The revisions, addition, and republications read as follows:

§ 312.6 Right 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:

* * * * *

(b) Where personal information is collected from the child pursuant to § 312.5(c)(10), the operator of the website or online service is required to provide the rights under paragraph (a) of this section to the school and is not required to provide such rights to a parent whose child has provided personal information to the website or online service.

(c) 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.

(d) 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.

* * * * *

■ 8. Revise § 312.8 to read as follows:

§ 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 children's personal information security program that contains safeguards that are appropriate to the sensitivity of the personal information collected from children and the operator's size, complexity, and nature and scope of activities. To establish, implement, and maintain a children's personal information security program, the operator must:

(1) Designate one or more employees to coordinate the operator's children's personal information security program;

(2) Identify and, at least annually, perform additional assessments to identify internal and external risks to the confidentiality, security, and integrity of personal information collected from children and the sufficiency of any safeguards in place to control such risks;

(3) Design, implement, and maintain safeguards to control risks identified through the risk assessments required under paragraph (b)(2) of this section. Each safeguard must be based on the volume and sensitivity of the children's personal information that is at risk, and the likelihood that the risk could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information;

(4) Regularly test and monitor the effectiveness of the safeguards in place to control risks identified through the risk assessments required under paragraph (b)(2) of this section; and

(5) At least annually, evaluate and modify the children's personal information security program to address identified risks, results of required testing and monitoring, new or more efficient technological or operational methods to control for identified risks, or any other circumstances that an operator knows or has reason to know may have a material impact on its children's personal information security program or any safeguards in place.

(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.

■ 9. Revise § 312.10 to read as follows:

§ 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 and not for a secondary purpose. When such information is no longer reasonably necessary for the purpose for which it was collected, the operator must delete the information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion. Personal information collected online from a child may not be retained indefinitely. At a minimum, the operator must establish, implement, and maintain a written children's data retention policy that sets forth the purposes for which children's personal information is collected, the business need for retaining such information, and a timeframe for deletion of such information that precludes indefinite retention. The operator must provide its written children's data retention policy in the notice on the website or online service provided in accordance with § 312.4(d).

■ 10. In § 312.11:

■ a. Republish (b) introductory text;

■ b. Revise paragraphs (b)(2), (d)(1) and (2), and (d)(3)(iii);

■ c. Add paragraph (d)(4);

■ d. Redesignate paragraphs (f) and (g) as paragraphs (g) and (h);
■ e. Add paragraph (f);
■ f. Revise newly redesignated paragraph (g); and
■ g. Republish newly redesignated paragraph (h).

The republications, revisions, and additions read as follows:

§ 312.11 Safe harbor programs.

* * * * *

(b) *Criteria for approval of self-regulatory program guidelines.* Proposed safe harbor programs must demonstrate that they meet the following performance standards:

* * * * *

(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.

* * * * *

(d) * * *

(1) By [DATE SIX MONTHS AFTER PUBLICATION OF THE FINAL RULE IN THE **FEDERAL REGISTER**], and annually thereafter, submit a report to the Commission that identifies each subject operator and all approved websites or online services, as well as any subject operators that have left the safe harbor program. The report must also contain, at a minimum:

(i) A narrative description of the safe harbor program's business model, including whether it provides additional services such as training to subject operators;

(ii) Copies of each consumer complaint related to each subject operator's violation of a safe harbor program's guidelines;

(iii) An aggregated summary of the results of the independent assessments conducted under paragraph (b)(2) of this section;

(iv) A description of each disciplinary action taken against any subject operator under paragraph (b)(3) of this section, as well as a description of the process for determining whether a subject operator is subject to discipline; and

(v) A description of any approvals of member operators' use of a parental consent mechanism, pursuant to § 312.5(b)(4);

(2) Promptly respond to Commission requests for additional information; and

(3) * * *

(iii) Results of the independent assessments of subject operators' compliance required under paragraph (b)(2) of this section; and

(4) No later than [DATE 90 DAYS AFTER PUBLICATION OF THE FINAL RULE IN THE **FEDERAL REGISTER**], publicly post a list of all current subject operators on each of the approved safe harbor program's websites and online services. 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.

* * * * *

(f) *Review of self-regulatory program guidelines.* Every three years approved safe harbor programs shall submit to the Commission a report detailing the safe harbor program's technological capabilities and mechanisms for assessing subject operators' fitness for membership in the safe harbor program.

(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.

(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.

■ 11. In § 312.12, revise paragraph (b) to read as follows:

§ 312.12 Voluntary Commission approval processes.

* * * * *

(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.

By direction of the Commission.

Joel Christie,

Acting Secretary.

[FR Doc. 2023–28569 Filed 1–10–24; 8:45 am]

BILLING CODE 6750–01–P