Comments of Consumer Reports
In Response to the
Federal Trade Commission
Notice of Proposed Rulemaking on the
COPPA Rule

By

Matt Schwartz, Policy Analyst

March 11, 2023

Consumer Reports[1] appreciates the opportunity to provide feedback on the Federal Trade Commission's (FTC) Request for Comment on its Notice of Proposed Rulemaking on the Children's Online Privacy Protection (COPPA Rule). We thank the Commission for initiating this proceeding and for its other efforts to rein in excessive commercial data practices.

This Rulemaking is an important step in ensuring that the FTC has updated authorities commensurate with rapid changes in technology and an evolving marketplace for children's data that conspire to create a moving target for the Commission's oversight of the Rule. Though the FTC has undertaken a handful of enforcement actions (e.g., Kurbo,[2] EPIC Games,[3] Microsoft,[4] and Amazon[5]) regarding alleged violations of the COPPA Rule since the initiation of this Rule Review in 2019, we continue[6] to believe the Commission can do more in light of apparently widespread noncompliance.[7] Stricter requirements guiding how companies may collect and share children's information are long overdue.

Below, we respond to questions posted in the Request for Comment, describing our views on the proposed updates to the COPPA Rule in detail.

---

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

[2] Federal Trade Commission, FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data, (March 4, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers-illegally-collecting-kids-sensitive

[3] Federal Trade Commission, Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges, (December 19, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations

[4] Federal Trade Commission, FTC Will Require Microsoft to Pay $20 million over Charges it Illegally Collected Personal Information from Children without Their Parents' Consent, (June 5, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-will-require-microsoft-pay-20-million-over-charges-it-illegally-collected-personal-information

[5] Federal Trade Commission, FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests, (March 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever

[6] Katie McInnis, *Consumer Reports Response to COPPA Rule Review, 16 CFR part 312, Project No. P195404,* Consumer Reports, (December 11, 2019), https://advocacy.consumerreports.org/wp-content/uploads/2019/12/COPPA-12.11.19-Consumer-Reports-1.pdf

[7] E.g. Narseo Vallina-Rodriguez, Serge Egelman, et al., Won't Someone Think of the Children? Examining COPPA Compliance at Scale, 3 PROCEEDINGS ON PRIVACY ENHANCING TECHNOLOGIES (PoPETS) 63-83, 63 (2018), https://blues.cs.berkeley.edu/wp-content/uploads/2018/04/popets-2018-0021.pdf

Responses to Commission Questions

Definitions

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?*

Consumer Reports supports the Commission's proposed revision to include mobile telephone numbers within the definition of "online contact information" so that operators may send text messages to initiate the verifiable parental consent (VPC) process. Businesses regularly cite the difficulty of obtaining VPC as one of the core burdens of the Rule and a major incentive to take advantage of the so-called "general audience loophole" whereby operators regularly claim ignorance on their audience composition in order to avoid compliance.[8] Allowing VPC requests to be initiated via text should mitigate at least some of these concerns and aligns with the expectations of many consumers who, in recent years, have grown more accustomed to managing account credentials and authentication via their mobile device.[9] While there may be a risk for increased fraud through this new mechanism (e.g. spoofed VPC requests that link to malicious sites or download malware), this risk doesn't seem appreciably stronger than with existing contact methods already included in the definition of "online contact information", such as email addresses.

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.Through the 2013 Amendments, the Commission defined personal information to include screen or user names only to the extent these 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*

---

[8] See, e.g., Future of Privacy Forum, The State of Play: Verifiable Parental Consent and COPPA at 33-34, https://fpf.org/wp-content/uploads/2021/11/FPF-The-State-of-Play-Verifiable-Parental-Consent-and-COPPA.pdf

[9] Chrysta Cherrie, 2FA Statistics: 2FA Climbs, While Password Managers and Biometrics Trend (noting a rising trend in survey respondents who have used two-factor authentication and that SMS was the most common second factor), Duo Labs (September 14, 2021), https://duo.com/blog/the-2021-state-of-the-auth-report-2fa-climbs-password-managers-biometrics-trend

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?

Screen or user names should be treated as online contact information, even if direct contact functions are not enabled on a given service. As the Commission correctly points out, it is often trivially easy to follow a user from one service to the next using screen or user names, which could allow another user to contact the child on a different service even if direct contact was not allowed on the first service. Treating screen or user names as online contact information provides important protections to that information, for example by requiring VPC prior to its collection and, given the the proposed revisions to § 312.7, tying it data minimization standards that prevent operators from requiring children to disclose more personal information than is reasonably necessary to participate in a game, offering of a prize, or another activity.

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?

Operators could of course institute internal rules that prevent users from taking screen or usernames that directly identify them (e.g. first and last name formats, addresses), though it is easy to imagine how those rules could easily be circumvented by creative uses of characters, hints, pseudonyms, or other methods. It is also hard to envisage how a single operator could prevent the scenario contemplated by the Commission of a child that consistently uses the same screen or user name being tracked across multiple services, any of which may offer direct contact methods. In the spirit of children's protection around which this Rule is clearly oriented, we'd suggest that the Commission take a broad view in construing screen or usernames as personal information, even though not all user or screen names may contain directly identifying personal information or allow direct contact.

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?*

Consumer Reports agrees with the Commission's interpretation in cases like *Microsoft* that biometric information is a category of "personal information"[10] and that biometric identifiers should be explicitly included as a category of personal information in the updated Rules. Biometric identifiers are routinely collected by many businesses, including some of the largest

[10] Lesley Fair, $20 million FTC settlement addresses Microsoft Xbox illegal collection of kids' data: A game changer for COPPA compliance, Federal Trade Commission Business Blog, (June 5, 2023) https://www.ftc.gov/business-guidance/blog/2023/06/20-million-ftc-settlement-addresses-microsoft-xbox-illegal-collection-kids-data-game-changer-coppa

online platforms[11] and are the most inherently personal information about an individual that exists.

Biometric data is included as a standard category of personal information in the growing number of state-level comprehensive privacy laws.[12] Indeed, biometric data under such laws is often deemed as a sub-category of personal information, "sensitive information", which is afforded additional protections, such as a heightened opt-in consent standard that applies to all individuals, not just children.[13]

We agree that all of the above-given categories of information (e.g. voice data, gait data) constitute examples of biometric identifiers and with the Commission's general approach of making the list of biometric identifiers non-exhaustive in order to allow for flexibility in the likely case of further technological developments on this front. We do not believe there is a need for additional exceptions. As a general principle, parents should know and have choice when operators want to collect or process data about their child's most personal attributes, even if such activities are ephemeral.

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?*

If the Commission's proposed addition of "biometric identifiers" to the definition of personal information is adopted, we believe that would encompass an avatar generated from the image of a child, since such an avatar would be constructed using "data derived from…facial data".[14] Even if that addition was not adopted, the likeness of a child generated from an image should constitute "personal information", since it could be used, alone or in combination with other information, to individually identify the child. The Commission could clarify this by adding "or likeness of a child" to the § 312.2, subparagraph 8 within the definition of "personal information."

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?*

---

[11] Ian Ducey, Biometric Data Collection And Big Tech: Imposing Ethical Constraints On Entities That Harvest Biometric Data, *Seattle Journal of Technology, Environmental & Innovation Law: Vol. 12: Iss. 2, Article 2,* (2022), https://digitalcommons.law.seattleu.edu/sjteil/vol12/iss2/2/

[12] As of this writing, all 14 comprehensive privacy laws include "biometric data" in their definition of personal information.

[13] See, e.g., Public Act No. 22-15, The Connecticut Data Privacy Act, Section 1(27), https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF

[14] Federal Trade Commission, Notice of Proposed Rulemaking on the Children's Online Privacy Protection Rule, Proposed § 312.2(10) at 2071, (January 11, 2024), [hereinafter FTC COPPA ANPR] https://www.federalregister.gov/documents/2024/01/11/2023-28569/childrens-online-privacy-protection-rule#footnote-366-p2069

The Commission should revise the definition so that government-issued identifiers are included as a category of personal information. Specific examples of government-issued identifiers that should be included in the definition, aside from Social Security numbers, are passports, birth certificates, and DMV-issued Child ID cards. It is Consumer Reports' view that such information should already be considered personal information under the Rule, but given the current stand-alone inclusion of Social Security numbers, more clarity would be helpful.

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?*

One important clarification we believe the Commission should make to this prong of the definition is to explicitly state that information "inferred" about a child is information "concerning the child." While the Commission states that it has decided not to propose including inferred data as "personal data" because the COPPA statute only pertains to the collection of personal information *from* a child,[15] we believe this is an unnecessarily narrow reading of the statute. These inferences are often merely an *extension* of the collection of personal information from a child and thus fall within the statute's purview. In other words, data inferences can only be created from the collection of information concerning a child; were it not for the operator's initial collection of information concerning a child, they would not be able to generate inferences to supplement that data.

Data inferred about a child is one of the riskiest types of data a business can have. Inferences are commonly used to sort individuals into marketing categories (e.g. big spenders), which are then used, sold, or shared with other third-parties for the purpose of targeting advertisements to them.[16] Because these inferences often occur without the consumers' knowledge, consumers often have very little transparency into how they might be categorized, let alone an ability to correct or delete such data if it is inaccurate. If disclosed, business' assumptions about a child carry the risk for personal embarrassment, social stigmatization, discrimination, could be used as a basis to make legal or other similarly significant decisions, or create other harms. Parents should have the right to be notified when this information is generated about their children and should have the ability to revoke their consent and delete this information. We note that derived data and inferences are increasingly included within the scope of privacy laws on the state level, including in the California Consumer Privacy Act[17] and Washington's new health privacy law.[18]

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*

---

[15] Id. at 2042
[16] See, e.g., Anne Longfield, Who Knows What About Me?, Children's Commissioner for England, (November 2018), https://assets.childrenscommissioner.gov.uk/wpuploads/2018/11/cco-who-knows-what-about-me.pdf
[17] CCPA Sec. 1798.140(v)(1)(K)
[18] Washington My Health, My Data Act, RCW 19.373.010(8)(b)(xiii)

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?

Under the current Rules, operators are exempt from their obligations to provide notice and receive VPC for the collection of personal information when the 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 Web site or online service."[19] One such permissible internal operation is activity necessary to "[a]uthenticate users of, or personalize the content on, the Web site or online service."[20] We agree with the idea that this exception is overly broad as written. In our view, while some degree of personalization based on data collected by the operator (e.g. personalized playlists of songs based on listening history) may be acceptable (especially to the extent it is reasonably expected by the user in the context of their interaction with the operator), some personalization goes too far and only exists to serve the operator's interests. In other words, operators *should* be able to use persistent identifiers to do things like save a child's progress in a game, preserve user privacy settings, or remember a character's skin or costume (i.e. actions the child reasonably expects and that are necessary for the core functionality of the service). The Commission's FAQs reflect that this is the Commission's current understanding of the purpose of this exception.[21] On the other hand, some operator driven personalization includes tactics like the creation of profiles of children that help businesses optimize the frequency or timing of notifications or nudges,[22] which clearly is not necessary for the core functionality of the service and thus should be subject to the Rule's notification and consent requirements.

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?*

The existing exemption for the use of persistent identifiers to serve contextual advertising is ambiguous and points to the need for greater clarity relating to the terms "contextual advertising" and "behavioral advertising" that are used in the Rule without definition. Contextual advertising is commonly understood to encompass advertising based on the content or nature of the website or service where the advertisement appears and that does not vary depending on who is viewing the advertisement. For example, a sugary cereal company may want to place advertisements on a child gaming site, due to the high-likelihood that their product appeals to the target audience of the website. This would constitute a contextual advertisement. Behavioral advertising is commonly understood to encompass advertising that is tailored based on known

---

[19] 16 C.F.R, § 312.5(c)(7)
[20] 16 C.F.R. § 312.2.
[21] Federal Trade Commission, Complying with COPPA: Frequently Asked Questions, J(8), (July 2020), https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions
[22] Ganapini and Panai, An Audit Framework for Adopting AI-Nudging on Children, Computers and Society, (April 25, 2023), https://arxiv.org/abs/2304.14338

or predicted preferences, characteristics, or interests associated with the individual who receives the advertisement. While we believe that the Rule's existing exception for the use of persistent identifiers to cap the frequency of contextual ads is reasonable, to the extent that advertisements are being "targeted" to individuals, that should constitute a behavioral advertisement that is not subject to the exception.

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?*

As an initial matter, Consumer Reports supports the Commission's proposed additions to the list of factors to be considered when determining whether a website or online service is directed to children, including the operator's marketing materials, representations to consumers and third-parties, and age of users on similar websites.

At the same time, we do not wish for the Commission to incentivize companies to collect *additional* data on consumers for the purpose of verifying age due to the potentially detrimental effects to privacy that such collection could engender. At the current moment, we do not believe there is a privacy preserving way of collecting, screening, or verifying the ages of all users (which would likely be necessary in order to determine the subset of child users) of a given service and would strongly caution against including any exceptions that would incentivize this type of behavior or indeed require it.

At the same time, operators should be incentivized to analyze any existing data they may have in order to determine their audience composition. Put another way, operators should *not* be rewarded for effectively burying their heads in the sand about the nature of their usership (as is the status quo now). For example, to the extent that a website or service already regularly undertakes behavioral analysis of their users that could reveal or produce a strong assumption

about the likely age of a user, they should be required to act on this information. As for what the cutoff should be in determining whether a website shall be deemed “directed to children” following such an analysis, we again suggest that the Commission take a broad view - perhaps whenever a business has more than 10 percent of child users and meets one of the other criteria set forth by the Commission.

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)?*

Given that the current Rule contemplates the direct notice of the operator's practices with regard to the “collection, use, or disclosure of personal information from children”[23], it tracks to require operators to share the identities or categories of those third parties to which data is shared or disclosed in such a notice. The third parties with which a operator shares personal data is likely one of the key decision points upon which parents evaluate their consent choices (for example, whether the operator shares personal data with social media companies or data brokers) and thus this type of information should be shared up-front in the direct notice, as well as in the online notice required under § 312.4(d). In recent years, Consumer Reports has advocated for privacy laws to require the disclosure of specific third parties with which covered entities share personal data on consumer transparency grounds, as well as the fact that such disclosures make assessing compliance easier for both regulators and consumer advocates.

Parental Consent

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?*

Consumer Reports applauds the Commission for taking the step to propose the bifurcation of consent processes such that parents would be able to consent to the collection of a child’s personal information but decline to consent to the disclosure of the child’s personal information to third parties. Under a consent-based model, it is crucial that a parent’s’ rights are not

[23] 16 CFR § 312.4(B)

presented to them in “all or nothing” fashion, such that a parent must accede to the sharing or selling of their child’s personal information in order for the child to be able to access the website or service. The Commission’s proposed change comports with the growing trend in privacy laws at the state level that similarly make it clear that consumers are allowed to deny unwanted secondary uses of personal data (e.g. sales, third-party targeted advertising, and profiling) but still retain access to the underlying product or service.[24]

Drawing from lessons learned from these privacy laws, we strongly urge the Commission to clearly prohibit businesses from attempting to “game” consent by bundling unrelated consents, misleading consumers about the effect of a consent decision, and manipulating consumers through consent interfaces to make the business’ preferred consent decision.

We would also suggest that the Commission clarify that a disclosure to a third-party is “integral” to the nature of the website or online service when it is functionally necessary to provide the product or service the consumer is asking for. For example, a video game platform that allows third-party brands to create virtual worlds should be able to disclose personal data to that brand necessary to allow that virtual world to load. On the other hand, the Commission should clarify that the sale or sharing of personal information for consideration (monetary or otherwise) shall never be considered “integral” to the nature of the website or service. For example, a business should be prohibited from ignoring its responsibility to receive VPC prior to disclosing personal data because it has claimed that the facilitation of targeted advertisements on its website is “integral” to the business because that is how they monetize the website.

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?*

While we are not positioned to speculate on operators’ compliance efforts with § 312.7, we are glad to see the Commission clarify its position that this provision should be viewed as a bonafide data minimization provision that “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” and that restricts operators from collecting superfluous data “even if the operator obtains consent for the collection of information that goes beyond what is reasonably necessary.”[25]

---

[24] IAPP, US State Privacy Legislation Tracker 2024 (see chart referencing that many states include a prohibition on discrimination based on the exercise of consumer rights), (2024), https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf

[25] Id.

As the Commission is aware, prevailing marketplace dynamics incentivize precisely the opposite behavior from operators. In 2022, social media companies in the United States alone generated $11 billion in revenue from advertising to minors.[26] Due to the lucrative nature of behavioral targeted advertising in particular, consumers' are persistently tracked both on and across websites and apps, and their online behavior is often combined with offline activities to provide detailed insights into their most personal characteristics, including health conditions, socioeconomic status, and preferences.

Given the Commission's interpretation of § 312.7, any child directed website that contains common types of third-party behavioral tracking (e.g. third-party cookies, the Facebook pixel) on a game, offering of a prize, or another activity would seem to be in violation (even if they have received VPC for such tracking), since, in our view, this type of tracking would never be reasonably necessary to allow the child to participate in the activity.

Relatedly, Consumer Reports strongly supports the Commission's proposed updates to § 312.10 (data retention), to clarify that operators must only "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**" (emphasis added) and that personal information may not be retained indefinitely. These retention provisions will ensure that the data minimization protections contemplated in § 312.7 extend beyond the collection phase so that operators may not use personal information for unexpected secondary purposes, like profiling or third-party targeted advertising. Ensuring the timely deletion of unneeded personal information will also reduce the attack surface for data breaches.

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?*

As detailed in our response to Question 14 (*supra),* Consumer Reports is supportive of a framework that would allow for disclosures of personal information when they are "reasonably necessary" to provide the service requested by the user.

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

The fact that information practices are *generally* disclosed to parents should not be deemed relevant, on its own, in assessing whether a *specific* information collection activity is reasonably necessary or not. As the Commission is aware, privacy notices are written to be vague and broad by design, so as to give the company maximum latitude to pursue its preferred current or future data collection and processing activities. In other words, companies are likely to grant

[26] Raffoul et al., Social media platforms generate billions of dollars in revenue from U.S. youth: Findings from a simulated revenue model, PLoS ONE 18(12), (December 27, 2023), https://doi.org/10.1371/journal.pone.0295337

themselves far more expansive data collection permissions than what is actually reasonably necessary to provide the service to the user.

The Commission's oversight of this provision should primarily involve a comparison of the operator's stated collection activities against what the Commission contextually assesses to be the data reasonably necessary to provide the service.

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"?*

Consumer Reports strongly recommends that the Commission adopt the revision as proposed. As the Commission has now clarified its interpretation of that provision, companies are now in turn likely to adopt a narrow reading of the term "activity" as to reduce the amount of data subject to this restriction. The Commission's proposed language that would clarify that "activity" means "any activity" offered by the website or online service even if the activity represents "the entirety of the website or online service" is therefore crucial to ensuring that the data minimization principle is applied broadly. At the same time, the proposed change should reduce the amount of guesswork required by companies to determine what "activities" would fall under the data minimization restriction and thus should also streamline compliance.

****

We thank the Federal Trade Commision for its consideration of these points, and for its work to secure strong privacy protections for consumers. We are happy to answer any questions you may have, and to discuss these issues in more detail. Please contact Matt Schwartz (matt.schwartz@consumer.org) or Justin Brookman (justin.brookman@consumer.org) for more information.