

March 11, 2024

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

Submitted via Regulations.gov.

Re: Children’s Online Privacy Protection Rule, Docket No. FTC-2024-0003; COPPA Rule Review, Project No. P195404



**National Political
Advocacy Department**
915 15th Street, NW, 6th Floor
Washington, DC 20005-2112
[aclu.org](https://www.aclu.org)

Deirdre Schifeling
Chief Political &
Advocacy Officer

Anthony D. Romero
Executive Director

Deborah N. Archer
President

The American Civil Liberties Union (ACLU) is pleased to submit these comments on the proposed rule by the Federal Trade Commission (Commission) regarding the Children’s Online Privacy Protection Act (COPPA).¹ For decades, the ACLU has championed the expressive rights of individuals using new technologies, while protecting against incursions on privacy those technologies might enable.²

In that vein, the ACLU has long supported robust privacy protections not only to protect our ability to speak, learn, and connect online but also to further models for federal comprehensive privacy legislation. For that reason, the “ACLU has long been strongly supportive of COPPA. It is an important first step on the road to universal baseline privacy protections that ensure that every American—young and old—has meaningful control over their personal information online.”³ And yet, well-meaning privacy legislation may overbroadly restrain the flow of information and individuals’ ability to speak, raising serious constitutional concerns and jeopardizing legislative efforts aimed at protecting privacy.⁴ The ACLU offers these comments in line with its commitment to *both* freedom of expression and privacy rights.

Below, the ACLU urges the Commission to further COPPA’s goals consistent with minors’ and adults’ freedom of expression by:

- Strengthening the proposal’s data minimization rules, while recognizing exceptions for internal operations to avoid unintended consequences.
- Accounting for First Amendment limitations on the regulation of speech online, including by formulating a more concrete proposal

¹ Children’s Online Privacy Protection Rule, 89 Fed. Reg. 2034 (Jan. 11, 2024), [here](#) (hereinafter “NPRM”).

² See *Video and Library Privacy Protection Acts of 1988: Hearing Before the Subcommittee on Technology and the Law* (Aug. 3, 1988) (statement of Janlori Goldman), [here](#).

³ Gabe Rottman, *FTC Proposes Changes to Privacy Law That Collide With Free Speech*, ACLU (Sept. 26, 2012), [here](#).

⁴ *E.g.*, *Sorrell v. IMS Health, Inc.*, 564 U.S. 552 (2011); *IMDB.com v. Becerra*, 962 F.3d 1111 (9th Cir. 2020).

regarding the indirect collection of personal information by third-party services.

- Avoiding technical and constitutional questions by declining to modify the statutory “actual knowledge” and “directed to children” standards and the long-standing treatment of age-verification under COPPA.
- Strengthening other provisions in the proposed rule to place the burden of protecting privacy on entities that collect children’s personal information.

I. The Commission Should Refine Its Proposed Data Minimization Rules to Strengthen Their Protections and to Avoid Unintended Consequences

A. The Proposed Rules Provide a Strong Foundation to Protect Children’s Privacy Through Its Expanded Data Minimization Rules



Responsive to Question 18.

The Commission appropriately underscores the role of data minimization in the current and proposed Rules, especially in §§ 312.7 and 312.10. However, as described below, those two provisions may be further strengthened while accommodating specific uses of personal information that are reasonably necessary for the operation of online services. Of particular importance are uses of data to support certain internal operations, such as for security or legal compliance.

“Data minimization” refers to the basic principle that an entity “should only create, collect, use, process, store, maintain, disseminate, or disclose [personal information] that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain [personal information] for as long as is necessary to accomplish the purpose.”⁵ Data minimization centers consumers’ reasonable expectations about the use of their information, such as limiting data collection and use to what “is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the individual.”⁶

In line with that basic principle, § 312.7 of the current Rule already prohibits “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.”⁷ As the Commission observes, “[T]his provision serves as an outright prohibition on collecting more personal information than is

⁵ *Fair Information Practice Principles (FIPPs)*, Federal Privacy Council, [here](#) (last visited Dec. 20, 2023).

⁶ American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 101(a)(1) (2022).

⁷ 16 C.F.R. § 312.7.



reasonably necessary 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.”⁸ Similarly, in § 312.10, the current Rule also prohibits retaining data for longer than “is reasonably necessary to fulfill the purpose for which the information was collected.”⁹ Data minimization protections such as these provisions advance critical privacy and cybersecurity goals.

The Commission’s proposal appropriately bolsters both of these protections.

First, proposed § 312.7 would clarify that an “activity” includes “any activity offered by a website or online service,” regardless of whether it is a single feature or component or the entirety of the website or service. This is the correct approach—limiting the Rule’s data minimization requirements to only specific features or components would eviscerate the promise of data minimization protections. Such limitations would place the onus of protecting privacy back on individuals instead of on operators, requiring individuals to vet whether *this* feature or *this* component provides adequate privacy protections. Instead, data minimization protections should reflect consumers’ expectations, regardless of whether the data was collected for a specific feature or function of a site or service.

Second, proposed § 312.10 would similarly limit operators’ use and retention of information. The proposed rule would limit retention of personal information to “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.” Secondary purposes are often improperly used to justify the indefinite retention of personal information, and the express prohibition on secondary purposes is essential for precluding the prolonged retention of children’s personal information. The additional proposal to expressly prohibit indefinite retention provides a bright-line rule that will help further this interest.

Proposed §§ 312.7 and 312.10 should be adopted by the Commissions, subject to the revisions below.

B. The Data Minimization Protections in §§ 312.7 and 312.10 Should Be Strengthened and Should Permit Uses to Support Internal Operations

Responsive to Question 17(b).

Both §§ 312.7 and 312.10 may be further refined to strengthen their protections and to avoid unintended consequences. To further strengthen

⁸ NPRM at 2060.

⁹ 16 C.F.R. § 312.10.

proposed § 312.7, the Commission should expand its prohibition beyond a child disclosing more information than is necessary and include the operator’s collection, processing, and retention of the information. Section 312.7 would read:

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 **disclosure of or the operator’s collection, processing, or retention of** more personal information than is reasonably necessary to participate in such activity, **except as is reasonably necessary for support for the internal operations of the Web site or online service.**



This amendment would close loopholes surrounding potential secondary *uses* of children’s personal information—possibly buried in privacy policies—beyond the “the child’s disclosing” of information. For example, the current limitation on a “child’s disclosing” of personal information does not reach subsequent uses by the operator; thus, a child might disclose their email address to register for a prize, and (under the current Rule) the operator would not be prohibited from using the email address for marketing, so long as it also obtained parental consent. The amended language proposed above would preclude that practice and further bolster the privacy and security of the information, consistent with the statute’s directive.¹⁰ To avoid unintended consequences, this language would still permit key uses of personal information for internal operations, such as for security or legal compliance.

Similarly, the Commission should consider additional measures both to strengthen § 312.10 and to avoid unintended consequences. Section 312.10 may be strengthened by limiting the “specific purpose(s)” to those that the individual—namely the child or parent—would reasonably expect. Section 312.10 would read:

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 **provide the service activity requested by the child** and not for a secondary purpose, **except as is reasonably necessary for support for the internal operations of the Web site or online service. . . .**

As with the amendment to § 312.7, this language would foreclose the use of information for purposes that are disclosed only in a privacy policy. Parents and children—like all people—should be able to assume that their information is being collected only for the service they are signing up for, and not some secondary purpose hidden in a privacy policy. Similarly, to avoid precluding uses that bolster privacy and security, the amended language would permit reasonable uses to support internal operations.

¹⁰ 15 U.S.C. § 6502(b)(1)(C).



Personal information governed by the amended language of both provisions would still be subject to the notice, consent, access, and deletion requirements of the Rule. As the Commission recognizes, the Rule's data minimization requirements apply "even if the operator obtains consent for the collection of information that goes beyond what is reasonably necessary."¹¹ That is, the data minimization protections are additive to the Rule's other provisions. Thus, nothing in the data minimization provisions relieves operators from their other obligations, and an operator will still be required to provide notice of and receive consent for the personal information they collect, process, and disclose for minors to participate in activities on the site or service; the same would be true for personal information used to support internal operations, unless an exception applies.

C. The Commission Should Reject Premising Any Data Minimization Protections on Disclosures in Privacy Policies or Other Notices

Responsive to Question 17(c).

Finally, in promulgating the final rule, the Commission should avoid approaches that achieve data minimization in name only. As noted above, the limitations imposed by data minimization rules should reflect consumers' reasonable expectations. Recent state legislation, however, limits the "collection of personal data" to purposes "disclosed to the consumer."¹² The net result of such an approach is that if an entity discloses the collection or processing of data, even in an opaque privacy policy, the collection or processing will be permissible. These are not meaningful protections, but business as usual.

In this vein, the Commission asks, "[T]o what extent should the Commission consider the information practices disclosed to the parent in assessing whether information collection is reasonably necessary?"¹³ This approach would essentially turn data minimization on its head, tying its protections not to consumers' reasonable expectations about the use of their information, but to uses that are disclosed in privacy policies. The Commission should avoid that approach.

II. The Final Rule Must Account for First Amendment Limitations on the Regulation of Speech Online

A. The Commission's Proposal to Regulate Third Parties that Indirectly Collect Personal Information Raises Constitutional Questions, and the Commission Should Consider a More Concrete Approach

¹¹ NPRM at 2060.

¹² *E.g.*, Conn. Pub. Act No. 22-15, sec. 6(a)(1) (2022); Del. Code Ann., tit. 6, § 12D-106(a)(1); Ind. Code § 24-15-4-1(1); Va. Code Ann. § 59.1-578(A)(1).

¹³ NPRM at 2071.



The Commission proposes to extend the definition of “Website or online service directed to children” in the COPPA Rule to operators that knowingly collect personal information from a child-directed service, even if they do not collect the information directly from the service’s users, such as “ad exchanges” that collect data from “an ad network,” which in turn collects from the users of a child-directed service.¹⁴

The expanded reach of the Commission’s proposal raises significant constitutional questions due to its regulation of a third party’s receipt and possession of information. Although courts have condoned regulating the *acquisition or collection* of information in certain circumstances,¹⁵ they have subjected restrictions imposed on the information’s subsequent recipients to “heightened judicial scrutiny.”¹⁶ For example, in *Bartnicki v. Vopper*, the Supreme Court concluded that a news broadcaster could not be punished for publishing a phone call provided to it by another party, because the broadcaster was not involved in its initial (illegal) recording and acquisition.¹⁷ The *Bartnicki* Court reasoned, “The normal method of deterring unlawful conduct is to impose an appropriate punishment on the person who engages in it. . . . But it would be quite remarkable to hold that speech by a law-abiding possessor [or recipient] of information can be suppressed in order to deter conduct by a non-law-abiding third party.”¹⁸ Similarly, the Court recognized in a related case, “An individual’s right to speak is implicated when information he or she possesses is subjected to ‘restraints on the way in which the information might be used’ or disseminated.”¹⁹ A third party’s mere receipt and possession of such information is protected,²⁰ as is a “request” for information, even if the information was improperly obtained originally.²¹

¹⁴ NPRM at 2047.

¹⁵ *Branzburg v. Hayes*, 408 U.S. 665, 691 (1972) (“Although stealing documents or private wiretapping could provide newsworthy information, neither reporter nor source is immune from conviction for such conduct, whatever the impact on the flow of news.”).

¹⁶ *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 567-68 (2011) (invalidating state-imposed “restriction on access to information in private hands”); *accord Bartnicki v. Vopper*, 532 U.S. 514, 529–30 (2001); *Smith v. Daily Mail Pub. Co.*, 443 U.S. 97, 103 (1979) (“[I]f a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order.”).

¹⁷ *Bartnicki*, 532 U.S. at 528; *accord Sorrell*, 564 U.S. at 568 (2011).

¹⁸ *Bartnicki*, 532 U.S. at 530.

¹⁹ *Sorrell*, 564 U.S. at 568 (2011). The Court has recognized that “the creation and dissemination of information are speech within the meaning of the First Amendment.” *Id.* at 570; *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 759 (1985) (credit report is “speech”).

²⁰ *New York Times Co. v. United States*, 403 U.S. 713 (1971); *accord Bartnicki*, 532 U.S. at 529–30 (2001).

²¹ *Democratic Nat’l Comm. v. Russian Fed’n*, 392 F. Supp. 3d 410, 435 (S.D.N.Y. 2019); Letter Brief of Amici American Civil Liberties Union, Freedom of the Press Foundation, and Foundation for Individual Rights and Expression, *In re Search Warrant Dated November 5, 2021*, Case No. 21-MC-00813, ECF No. 140 at 7 (S.D.N.Y. June 2, 2023) (“Amici urge this Court to affirm that the First Amendment



As in *Bartnicki* and its progeny, the Commission’s proposal seeks to regulate a third party’s receipt and possession of information. Although the Commission cites concerns with the use of children’s information in the “online advertising ecosystem,” the proposed change would reach far more broadly. For example, the proposal would feasibly reach an online news site that discusses posts on a child-directed service. Under the Commission’s proposal, that news site would be subject to COPPA’s restrictions and would face a choice to obtain verifiable parental consent, not publish the information, or risk an enforcement action by the Commission. As in *Bartnicki*, the “normal method” of deterring unlawful uses of children’s personal information is to impose sanctions on the initial collection by the child-directed service, not on the newspaper that subsequently obtains the information.

However, a more narrowly tailored and more concrete proposal by the Commission may satisfy First Amendment scrutiny. The *Bartnicki* decision expressly depended on the fact that the speech involved a “matter of public concern” and the Court declined to “answer categorically whether truthful publication may ever be punished consistent with the First Amendment.”²² Similarly, the Court has applied a lower level of scrutiny for regulation of “speech on matters of purely private concern . . . solely in the individual interest of the speaker and its specific business audience,” such as consumer credit reports.²³ A more narrowly tailored proposal focused on ad exchanges or ad networks may satisfy those lower standards. Similarly, if the Commission is concerned about misuse of personal information by service providers or other third parties, the Commission may consider further bolstering the provisions in § 312.8 to ensure that operators take sufficient measures to commit those other entities to protecting children’s personal information.

*B. Restrictions on Contextual Advertising that Do Not Depend on
Collecting or Processing Personal Information Are Not Tailored to the
Interest Underlying COPPA*

Responsive to Question 10.

The Commission asks if it should consider changes to the Rule’s treatment of contextual advertising, explaining, “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.” Unfortunately, the preamble to the proposed rule does not

protects a reporter’s right to receive and possess documents on matters of public concern that were unlawfully obtained or disclosed by a third party.”).

²² *Bartnicki*, 532 U.S. at 529, 535.

²³ *Dun & Bradstreet*, 472 U. S. at 759-62; *Trans Union Corp. v. F.T.C.*, 245 F.3d 809, 818 (D.C. Cir. 2001) (credit reports were “solely in the interest of the speaker and its specific business audience”).



explain the data practices contemplated by this question, and without that context, it is difficult to provide meaningful comments.

At baseline, contextual advertising should—by definition—be neither using personal information nor “targeted” to individuals. Although there is no standard definition of “contextual advertising,” most conceptions of the practice note that it does not rely on personal information. For example, last Congress’s American Data Privacy and Protection Act defined contextual advertising as “when an advertisement is displayed based on the content in which the advertisement appears and does not vary based on who is viewing the advertisement.”²⁴ By definition, then, contextual advertising should only involve personal information to the extent necessary to deliver any content to a device²⁵—which would fall comfortably within the Rule’s exception for “support for internal operations.” Further, when a persistent identifier is collected to deliver content such as a contextual ad, the operator is limited by both the current and proposed COPPA Rule from using it for other purposes. Rather than relying on personal information, contextual advertising instead relies on information about sites and services, and regulating “contextual advertising” in this narrow sense would likely extend beyond the governmental interest underlying COPPA.²⁶

However, to the extent that advertising networks are using personal information beyond a persistent identifier such as browsing history to deliver advertising, that use likely falls outside COPPA’s “internal operations” exception and is likely subject to the Rule. The Commission should consider whether existing provisions may reach that conduct.

C. The Commission Should Ensure that Measures to Delete Children’s Information in the Private Messaging Space Do Not Unreasonably Intrude on User Privacy, Including in Its Approach to Screen Names

Responsive to Questions 2 and 4.

²⁴ American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 2(34)(B)(ii) (2022).

²⁵ See *What Is Contextual Advertising? Why Is It Important?*, Publift (Jan. 15, 2024), [here](#) (“[Ads] are displayed on the basis of where the user currently is instead of focusing on where the user has been.”); *AwesomeAds Marketplace Privacy Policy*, SuperAwesome (Apr. 24, 2023), [here](#) (processing is limited to “user agent string, IP address and the app’s BundleID” or site’s web domain address); *About Contextual Advertising*, Google Ads Help, [here](#) (last visited Feb. 20, 2024) (contextual advertising “consider[s] factors such as” text, language, link structure, and page structure of webpage or URL).

²⁶ Advertising is protected First-Amendment speech, and its regulation must be narrowly tailored to an important governmental interest. *Thompson v. Western States Medical Center*, 535 U.S. 357 (2002); *Lorillard Tobacco Co. v. Reilly*, 533 U.S. 525, 534-36 (2001); *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484 (1996).



The current COPPA Rule currently provides that an operator will not have “collected” a child’s personal information “if it takes reasonable measures to delete all or virtually all personal information from a child’s postings before they are made public.”²⁷ The Commission asks if that exception should apply to one-to-one communications.

The ACLU takes no position on the proposed change but urges the Commission to ensure that the proposal (if implemented) does not undermine user privacy. On one hand, the current Rule permits operators to remove children’s personal information from one-to-one messaging, thus allowing known children and users of child-directed services to engage in additional forms of communication, speech, and learning. On the other hand, such measures likely require the monitoring of users’ messages and may pose technical difficulties when implemented alongside privacy-protective measures such as end-to-end encryption.

Given the countervailing speech and privacy interests, the ACLU urges the Commission to ensure that the final Rule preserves privacy and user choice:

- First, because the removal of personal information may require monitoring users’ messages and may undermine end-to-end encryption, the Commission should reiterate that it is not requiring the removal of personal information from posts but that such removal is merely one option for complying with the COPPA Rule.
- Second, the Commission should strongly recommend or even require operators to notify users when the operator has opted to remove personal information from posts. Because the removal of personal information may necessitate monitoring or disabling privacy measures such as encryption, users should have easily digestible notice when such measures are in place.

The Commission also seeks comment on whether the use of screen names across services may “allow[] other users to contact and engage in direct communications with children on another online service.”²⁸ Even on a single platform, screen names often allow users to be identified and contacted, and users may include personal information in their screen name. For example, in one Pew Research survey, 82% of 18-29 year olds reported “post[ing] content online using some type of screen name *that people associate with them*.”²⁹ Further, in that same survey, 70% of all social media users post with their real names and 74% report posting with a dedicated screen name that people associate with them.³⁰ Another study found that users view screen names as having median sensitivity, concluding, “[R]espondents suggest that their online screen name is more sensitive than demographic characteristics (e.g.,

²⁷ 16 C.F.R. § 312.2 (definition of “collect”).

²⁸ NPRM at 2070.

²⁹ Mary Madden, *Most Would Like to Do More to Protect their Personal Information Online*, Pew Research Center (Nov. 12, 2014) (emphasis added), [here](#).

³⁰ *Id.*

one's race) and less sensitive than other personally-identifiable data that can be linked to an individual and her behavior (e.g., one's driver's license number)."³¹

Consequently, the Commission should continue to treat screen names as it does other personal information.³² For known children or users of child-directed sites, the screen name should be included as part of the notice-and-consent process; if consent is not obtained, the screen name should be subject to procedures to remove personally identifying information, such by providing randomized user names, a practice already employed by some child-directed services.³³

III. The Commission Is Appropriately Cautious in Declining to Modify the “Actual Knowledge” and “Directed to Children” Standards

A. *Alternatives to “Actual Knowledge” May Lead to Increased Data Collection and Have Not Been Fully Developed*

The Commission previously considered adopting an interpretation of “actual knowledge” that would include “constructive knowledge.”³⁴ The ACLU applauds the Commission’s decision not to pursue that interpretation.

A “constructive knowledge” interpretation would conflict directly with Congress’s express direction that COPPA apply when an operator has *actual* knowledge of a child’s age.³⁵ More concerning, “constructive knowledge” is vague and may lead to increased data collection as online services seek to comply with its broad scope. For example, “constructive knowledge” may include some form of imputing knowledge that another in the same position could or should have known.³⁶ This broad scope incentivizes platforms to collect as much information on users as possible to avoid being deemed responsible for information about which they were not actually aware.

Moreover, the exact contours of a constructive knowledge standard are far from clear, and its meaning could differ wildly based on platforms’ data collection practices. Although the Commission might delineate the

³¹ Libby Hemphill et al., *Comparative Sensitivity of Social Media Data and Their Acceptable Use in Research*, 9 Scientific Data 643 (2022), [here](#).

³² See 16 C.F.R. § 312.2 (“personal information” includes a “screen or user name where it functions in the same manner as online contact information, as defined in this section”).

³³ E.g., *Can I Change My Nickname After Activating My Account*, Lego, [here](#) (last visited Mar. 5, 2024) (“In our apps and games for kids, we give all new users a fun and anonymous nickname. Kids can select another nickname once every 30 days. You have to be 13 or older to have a personalized nickname.”).

³⁴ NPRM at 2037.

³⁵ 15 U.S.C. § 6502(a)(1), (b)(1).

³⁶ Knowledge, Black’s Law Dictionary (11th ed. 2019) (providing, as an example, “the court held that the partners had constructive knowledge of the partnership agreement even though none of them had read it”)



boundaries of a “constructive knowledge” standard over time, the Supreme Court has rejected such incremental development of standards regulating speech and information, as the intervening indeterminacy “must necessarily chill speech.”³⁷

Further, a “constructive knowledge” standard would mean that the platforms that track, surveil, and profile us *the most* would be the best situated to identify who is a child and adhere to COPPA’s requirements. Not only would that tilt the regulatory field in favor of entrenched incumbents, but it would perversely enshrine their invasive surveillance as a “privacy” “protection” measure.



Finally, a constructive knowledge standard is unnecessary. As the Commission notes, “actual knowledge includes willful disregard.”³⁸ Thus, entities that “willfully blind” themselves to known facts regarding a users’ age are still within the existing standard’s scope. The Commission has also demonstrated in recent enforcement actions that it is prepared to find a service “directed to children” if the operator actively targets child users, including through marketing or publicity, while ignoring empirical evidence regarding substantial numbers of children using the service.³⁹

B. The Commission Should Avoid Mandating Age Verification Because It Is a Barrier to Speech

Similarly, the Commission should avoid mandating age verification and the serious constitutional issues it raises.⁴⁰ Since the passage of the Communications Decency Act in 1996, courts have consistently held that age verification requirements imposed on speech intermediaries online are unconstitutional.⁴¹ And for good reason: age verification requirements impermissibly burden both children’s and adults’ access to constitutionally protected speech.⁴² In addition, age verification demands additional data collection and subsequently invades individuals’ privacy.⁴³ Those privacy

³⁷ *Riley v. Nat’l Fed’n of the Blind of N.C., Inc.*, 487 U.S. 781, 797-98 (1988) (measure requiring speaker to prove “reasonableness” was too vague and “must necessarily chill speech” and could not be “judicially defined over the years”).

³⁸ NPRM at 2037 n.46.

³⁹ Complaint ¶¶ 22-35, *United States v. Epic Games*, No. 22-cv-518, ECF No. 1 (Dec. 19, 2022) (sending “swag” to children, presenting children’s usage to partners, and entering branding agreements with toy companies); Complaint ¶¶ 23-27, *FTC v. YouTube*, No. 19-cv-2642, ECF No. 1 (Sept. 4, 2019) (presenting children’s usage to marketing partners and creating a child-specific application).

⁴⁰ See NPRM at 2052 n.209.

⁴¹ *E.g.*, *Ashcroft v. ACLU*, 542 U.S. 656, 667 (2004); *Reno v. ACLU*, 521 U.S. 844, 855, 881-82 (1997).

⁴² *Ashcroft*, 542 U.S. at 667 (describing adults’ right to “access to speech they have a right to see without having to identify themselves”);

⁴³ Taylor Barkley, *Poll: Americans Don’t Want to Share Their Photo ID to Tweet*, The Center for Growth and Opportunity at Utah State University (Feb. 1, 2023), [here](#) (“2



incursions occur whether the verification takes place through a scan of your government ID by a third party, querying data provided by a data broker or credit agency, or deploying facial analysis technology.⁴⁴ Such data collection undermines not only goals to protect privacy but also individuals' rights to anonymity, and recent court decisions have emphasized that purported developments in age verification technology have not lessened the technology's intrusion on individuals' constitutional rights.⁴⁵

For those reasons, age verification should not be mandated for compliance with COPPA. Indeed, as the Commission has recognized for a quarter century,⁴⁶ COPPA does not mandate collection of age data. Instead, COPPA's ingenuity is that it is triggered by services' conduct—namely, their active targeting of minors.⁴⁷ This approach has avoided the technical and constitutional complications posed by age verification requirements, and we urge the Commission to maintain that long-standing approach in this rulemaking and in its future interpretation and enforcement of the COPPA Rule.

C. Alternatives to the Current “Directed to Children” Standard Would Sweep Up Large Portions of the Internet, Beyond the Scope Intended by Congress

Similarly, proposed alternatives to COPPA's existing “directed to children” standard, such as sites “likely to be accessed by children,” would sweep up general audience websites, including news, sports, and games. As with COPPA's knowledge standard, alternatives to the “directed to children”

out of 3 of Americans are not comfortable sharing their identification document with social media companies . . . 2 out of 3 Americans are not comfortable sharing their biometric information with platforms.”); Ofcom & Information Commissioner's Office, Families' Attitudes Toward Age Assurance (2022), [here](#) (“Most families felt hard identifiers would be more effective than self-declaration but had concerns over the information that this involved sharing. . . . Some parents and children felt uneasy about having to share their face with a website.”).

⁴⁴ Future of Privacy Forum, Unpacking Age Assurance: Technologies and Tradeoffs (2023), [here](#).

⁴⁵ NetChoice v. Griffin, No. 23-cv-5105 (W.D. Ark. Aug. 31, 2023), [here](#).

⁴⁶ 64 Fed. Reg. 59888, 59889 (Nov. 3, 1999), [here](#).

⁴⁷ Complaint ¶¶ 22-35, United States v. Epic Games, No. 22-cv-518 (Dec. 19, 2022) (sending “swag” to children, presenting children's usage to partners, and entering branding agreements with toy companies); Complaint ¶¶ 23-27, FTC v. YouTube, No. 19-cv-2642 (Sept. 4, 2019) (presenting children's usage to marketing partners and creating a child-specific application); NetChoice v. Yost, No. 24-cv-47 at 19 (D.C. Ohio Feb. 12, 2024), [here](#) (concluding that the “targeted to children” standard might consider content but is not a content-based regulation); cf. City of Austin v. Reagan Nat'l Advert. of Austin, LLC, 596 U.S. 61, 69 (2022), LLC, 596 U.S. 61, (2022) (“That does not mean that any classification that considers function or purpose [of speech] is always content based.”); Hill v. Colorado, 530 U.S. 703, 721 (2000) (“It is common in the law to examine the content of a communication to determine the speaker's purpose.”).

standard would run afoul of the statute’s plain language and congressional intent. The ACLU supports the Commission’s decision not to modify the Rule in this manner.⁴⁸

IV. Additional Protections in the Proposed Rule Should Place the Burden of Protecting Privacy on the Entities that Seek to Profit from Collecting and Processing Personal Information

A. Biometrics Are Highly Sensitive Information, and the Commission Should Avoid Broad Exceptions for “Prompt Deletion” that Would Permit Their Use Without Notice and Consent

Responsive to Question 5.



The ACLU supports the Commission’s proposal to include biometrics as “personal information” subject to the Rule. As the ACLU has repeatedly observed,⁴⁹ biometrics are inherently personally identifying and generally immutable. Consequently, biometrics pose marked threats to privacy, civil rights, and civil liberties. Those threats may include a loss of anonymity in contexts where people have traditionally expected it, persistent tracking of movement and activity, and identity theft. Additionally, flaws in the use or operation of biometric technologies can lead to false arrests and denial of access to benefits, goods, and services. These problems disproportionately affect people of color and members of other marginalized communities.⁵⁰ In light of those risks, the ACLU has supported robust privacy protections for biometrics and cautioned against or actively opposed their use in critical contexts like law enforcement, immigration, and governmental benefits. The Commission’s proposal would not only help mitigate those harms but also bring the COPPA Rule in line with other privacy laws, especially the Family Education Rights and Privacy Act.⁵¹

⁴⁸ NPRM at 2036.

⁴⁹ Comments of the ACLU and EPIC, Digital Identity Guidelines: Enrollment and Identity Proofing, Initial Public Draft, NIST SP 800-63A-4 IPD (April 14, 2023), [here](#); Comments of the ACLU, Commercial Surveillance ANPR, Docket No. FTC-2022-0053-0001 (Nov. 21, 2022), [here](#); Jay Stanley & Olga Akselrod, *Three Key Problems with the Government’s Use of a Flawed Facial Recognition Service*, ACLU (Feb. 2, 2022), [here](#); Comments of the ACLU, Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, Doc. No. 2021-21975 (Jan. 14, 2022), [here](#); Comments of the ACLU et al., Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States, Docket No. USCBP-2020-0062 (Dec. 21, 2020), [here](#); Comments of the ACLU et al., Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, Docket No. USCIS 2019-0007 (Oct. 13, 2020), [here](#).

⁵⁰ Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act at 5 (2023), [here](#).

⁵¹ 34 C.F.R. § 99.3 (including “biometric record” in the definition of “personally identifiable information”).



In implementing this proposal, the Commission should retain the current language covering biometrics that “can be used” for the “recognition of an individual,” which appropriately classifies the data based on its potential harmful future uses.⁵² In contrast, the Commission should eschew language that would limit the provision to identifiers that “are used” for the recognition of an individual. That latter approach does not cover biometrics that are not currently used for identification, even though they may be used for that purpose later.

The Commission also seeks comment on whether it should establish an exception to the Rule “for biometric data that has been promptly deleted.”⁵³ Although prompt deletion can further both privacy and security for personal information, an exception for prompt deletion of biometric is not ripe for inclusion in the Rule at this time.

An exception for prompt deletion of biometrics would be appropriate if two conditions were true: providing notice and obtaining consent would essentially eviscerate the benefits of using biometrics, *and* prompt deletion would largely eliminate the privacy risks in the biometrics’ collection and use. These conditions were underscored in the Commission’s 2017 “non-enforcement policy” regarding the prompt deletion of children’s voice recordings. There, the Commission exempted from the Rule voice recordings used “as a replacement for written words in performing search and other functions on internet-connected devices.”⁵⁴ As the Commission observed in that policy guidance:⁵⁵

Nevertheless, the Commission recognizes the *value of using voice as a replacement for written words in performing search and other functions* on internet-connected devices. Verbal commands may be a necessity for certain consumers, including children who have not yet learned to write, or the disabled. In addition, when the operator only uses the audio file as a replacement for written words, such as to effectuate an instruction or request, and only maintains the file long enough to complete that purpose and then immediately deletes it, *there is little risk the audio file will be used to contact an individual child.*

The record does not currently suggest additional uses of biometrics that would meet both of those conditions. Other common uses of biometrics to unlock a device, to identify individuals in photos, or to recognize users

⁵² See ACLU, State Biometric Identifiers Privacy Act Model Bill § 3(A), at 2 (2022), [here](#).

⁵³ NPRM at 2042.

⁵⁴ Federal Trade Commission, Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings 2 (2017), [here](#).

⁵⁵ *Id.* (emphasis added).



already require an initial process to set-up the feature or to opt-in.⁵⁶ In those instances, obtaining parental consent would be practicable for operators subject to the Rule, and there is no reason to broadly exempt biometrics at this time.

However, to address beneficial uses of biometrics that may emerge later, the Commission could consider adding an additional voluntary approval process to § 312.12, paralleling those for new parental consent methods or new supports for internal operations. A new provision in § 312.12 might state:

(c) **Prompt deletion of biometrics.** An interested party may file a written request for Commission approval of an exception for the collection of a biometric identifier as described in § 312.2 if the operator only maintains the biometric identifier long enough to complete the purpose for which it was collected and then immediately deletes it. To be considered for approval, a party must provide a detailed analysis of why providing notice and obtaining consent to collect the biometric identifier is impracticable and whether immediate deletion sufficiently mitigates the privacy risks in the biometric identifiers' collection and use. 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.

Creating exceptions to the Rule's protections for biometrics should be done on a case-by-case basis with a robust factual record; it is thus better suited for the voluntary approval process rather than ordinary rulemaking.

B. Permissible "Education Purposes" for School Authorization Should Exclude Loopholes Abused for Commercial Purposes

Responsive to Question 16.

The Commission should clarify that school authorization does *not* permit operators to "presume that the school's authorization is based on the school having obtained the parent's consent"⁵⁷ for commercial purposes. The Commission has long permitted schools to provide consent for uses of children's personal information in the educational context, variously describing the school as "agents" that consent on behalf of parents or mere "intermediaries" that actually obtain the necessary parental consent.⁵⁸

⁵⁶ *E.g., About Face ID Advanced Technology*, Apple, [here](#) (last visited Feb. 27, 2024) ("To start using Face ID, you need to first enroll your face."); *Search by People, Things & Places in Your Photos*, Google, [here](#) (last visited Feb. 27, 2024); *Turn on Voice Recognition with Voice Match*, Google, [here](#) (last visited Feb. 27, 2024).

⁵⁷ Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions* § N.1 (2020), [here](#).

⁵⁸ 64 Fed. Reg. 59888, 59903 (Nov. 3, 1999).



Operators, however, have abused this latitude to enable commercial uses of children’s personal information by presuming that schools have obtained parental consent, whether or not that presumption is true.⁵⁹ Operators have been successful in persuading at least one court that such a presumption permits commercial uses of children’s information; that court concluded:⁶⁰

The State argues the FTC guide clearly states that if an operator intends to use or disclose children’s personal information for its own commercial purposes in addition to the provision of services to the school, it will need to obtain parental consent. That is undisputed; however, it is equally undisputed that the FTC expressly recognizes intermediaries in functioning to obtain parental consent on behalf of operators such as Google. Ultimately, the law only requires “any reasonable effort” in providing notice to and obtaining consent from parents and, given that schools can provide notice in the scenario when personal information is collected for the use and benefit of the school, *it seems persuasive that schools can obtain consent as an intermediary for the scenario when information is also collected by the operator for other commercial purpose.*

In the proposed rule, the Commission’s intent may be to preclude *any* commercial uses of information obtained through school authorization by requiring written agreements to “[limit] the operator’s use and disclosure of the personal information to a school-authorized education purpose only and no other purpose.”⁶¹ That broad language could conceivably preclude commercial uses of personal information, even if the operator “presumes” that the school is acting as an intermediary that actually obtains parental consent. If that is the case, the ACLU supports this revision.

However, the proposed rule might also be read as limited to cases where school “authorization” is provided in the school’s role as an “agent” acting on behalf of parents—leaving in place the Commission’s existing guidance that schools may act as intermediaries. Given the Commission’s past recognition of schools functioning as “intermediaries”⁶² and some courts’ interpretation of that guidance,⁶³ the Commission should unequivocally state in the preamble to the final Rule that, regardless of whether the school functions as an intermediary or an agent, commercial uses of children’s personal information are not permitted. That is, even where an operator *presumes* that the school obtained parental consent in its role as an intermediary, no personal information collected by virtue of the school relationship may be used for non-educational purposes. The Commission should expressly reject operator’s reliance on schools as “intermediaries” for commercial uses of children’s

⁵⁹ New Mexico ex rel. Balderas v. Google, LLC, 489 F. Supp. 3d 1254, 1262 (D.N.M. 2020).

⁶⁰ *Balderas*, 489 F. Supp 3d at 1262 (emphasis added).

⁶¹ NPRM at 2075.

⁶² 64 Fed. Reg. at 59903.

⁶³ *Balderas*, 489 F. Supp 3d at 1262.

personal information in the preamble to the final Rule and in its FAQs on COPPA.

Alternatively, if the Commission wishes to retain schools' role as "intermediaries"—even for commercial uses of personal information—it should make the requirements described in its recent *Edmodo* complaint explicit in the Rule.⁶⁴ In the complaint, the Commission alleged that the operator could not rely on a school as an "intermediary" in actually obtaining parental consent, because the operator "failed to adequately inform schools and teachers of their role as intermediaries, failed to provide them with the information necessary for them to act as intermediaries, and failed to monitor whether parents ultimately actually provided verifiable consent."⁶⁵



The Commission might amend proposed § 312.5(c)(10) to make those requirements explicit:

(10) Where the operator obtains school authorization for the collection of the child's personal information for a school-authorized education purpose **or relies on the school as an intermediary to actually obtain verifiable parental consent**. 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 **or agreeing to serve as an intermediary** and attests that the person has the authority to do so;

(ii) **In the case of school authorization, limits** the operator's use and disclosure of the personal information to a school-authorized education purpose only and no other purpose, **and 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;

(iii) **In the case of the school serving as an intermediary in actually providing notice and obtaining verifiable parental consent as required by this part, clearly states the school's role as an intermediary, provides the disclosures required by this part, describes how the operator will monitor and verify that verifiable parental consent has been obtained, and states the operator will provide parents the rights required by this part; and,**

⁶⁴ Complaint ¶¶ 28, 42-53, *United States v. Edmodo*, No. 23-cv-2495, ECF No. 1 (May 22, 2023).

⁶⁵ *Id.* ¶ 28.

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

Similarly, the Commission should correspondingly adjust § 312.4(c)(5):

(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 **or actual obtaining of verifiable parental 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 school does not provide such authorization **or does not actually obtain verifiable parental consent**;

(ii) That the operator's use and disclosure of personal information collected from the child is limited to a school-authorized education purpose **or as authorized by verifiable parental consent actually obtained by the school**;

(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 **or obtain verifiable parental consent**;

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

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

(vi) **In the case of school authorization, the** means by which the school can authorize the collection, use, and disclosure of the information.

C. The Commission Should Require Operators to Separately Obtain Parental Consent for Disclosures of Children's Personal Information and Ensure that Parents May Obtain a List of Each Individual Recipient

Responsive to Question 14.





The COPPA Rule currently requires operators to give parents to “the option to consent to the collection and use of the child’s personal information without consenting to [its] disclosure.”⁶⁶ To effectuate that provision, the Commission has proposed a new paragraph in the Rule that will require a separate consent to the disclosure of children’s personal information, “except where such disclosure is integral to the nature of the website or online service.”⁶⁷

The ACLU supports this proposal, as it has supported opt-in regimes for other uses of private information.⁶⁸ Notice and consent requirements merely lead companies to bury their data practices in opaque privacy policies and do not provide individuals with meaningful information about the uses of their information or meaningful control over those uses.⁶⁹ Even where individuals can navigate disclosures in privacy policies, the interfaces to control uses of information are plagued with “dark patterns” designed to frustrate user choice.⁷⁰

The proposed rule would cure that shortcoming, at least in part. By mandating a stand-alone consent provision, the Commission is effectively requiring operators to obtain parental “opt-in” to the disclosure of children’s information.

Several factors inform how the Commission should implement a separate “opt-in” process for disclosures of personal information. In most cases, notice and consent processes should ideally be provided in approachable, “just-in-time” notices that are immediately proximate to the features or functions to which they relate.⁷¹ However, such notices would substantially alter established practice under COPPA, making a “just-in-time” notice possibly a poor fit. Thus, the “opt-in” for disclosures should be included during the normal course of obtaining parental consent. Likewise, the direct notice provided to parents is intended to be brief and approachable, making it impractical for the opt-in notice to name individual recipients of disclosures.

⁶⁶ 16 C.F.R. § 312.5(a)(2); *accord* COPPA FAQs, Federal Trade Commission sec. I.9 (2020), [here](#).

⁶⁷ NPRM at 2049.

⁶⁸ ACLU, State Biometric Identifiers Privacy Act Model Bill § 4(E)(1), at 6-7 (2022), [here](#) (“A private entity may not . . . [c]ondition the provision of a good or service on the collection, use, disclosure, transfer, sale, retention, or processing of biometric identifiers”); Brief of Amici Curiae ACLU et al., *ACA Connects v. Frey*, No. 20-cv-55, ECF No. 33 (May 29, 2020), [here](#) (urging court to uphold state law requiring opt-in consent prior to uses of personal information by broadband providers).

⁶⁹ Claire Park, *How “Notice and Consent” Fails to Protect Our Privacy*, New America (Mar. 23, 2020), [here](#); cf. Robert Gellman, *Is There a Role for Consent in Privacy?*, IAPP (June 30, 2021), [here](#).

⁷⁰ Staff Report, Federal Trade Commission, A Look at What ISPs Know About You 39-41 (2021), [here](#).

⁷¹ Information Commissioner’s Office, *The Right to Be Informed* 53 (2022), [here](#); Federal Trade Commission, *Mobile Privacy Disclosures* 15 (2013), [here](#).



Thus, in integrating consent for disclosures into the normal course of COPPA's notice and consent process, the Commission should ensure that the notice is clear and conspicuous. To ensure the notice is easily understood, it should state the categories of personal information that may be disclosed, the categories of recipients, and the purposes of the disclosures, without naming specific recipients. To effectuate those requirements, paragraph (iv) proposed by the Commission in § 312.4(c) could state:

(c) This direct notice shall set forth:

* * *

(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), **the specific categories of personal information disclosed**, the purposes for such disclosures, 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, **provide that such information shall be clearly and conspicuously set forth separately from the remainder of the direct notice**;

Although the brevity of the direct notice may limit the practicality of listing each individual recipient of a child's personal information, parents should still have access to that information. Several laws passed at the state level in recent years do not provide substantive limits on entities' use of personal information, but they do codify rights to access, correct, and delete information those entities have collected. Requiring operators under COPPA to identify specific recipients of children's personal information may help parents exercise their data rights under those other laws. To effectuate this, § 312.3(c) could be amended as follows:

(c) Provide a reasonable means for a parent to review the personal information collected from a child, **the specific personal information disclosed to third parties and the identify of each individual recipient (§ 312.5)**, and to refuse to permit its further use or maintenance (§ 312.6);

D. The Commission Should Maximize User Control of Profiling-Based Personalization and Consider Enforcement Actions as Appropriate for Push Notifications

Responsive to Questions 9 and 15.

The Commission seeks comment on whether it should reconsider permitting uses of personal information for "personalization" and push notifications under the "internal operations" and "multiple contacts" exceptions to the



Rule, respectively.⁷² Concerns about content personalization and push notifications have animated recent debates about children’s relationship with technology.⁷³ Unfortunately, recent proposals would directly regulate speech online,⁷⁴ rather than empowering users with control of their experiences—an approach that would more likely pass constitutional muster.⁷⁵

The Commission should seek to empower users with control over “personalization” of their online experiences, and it has the statutory authority to exclude personalization from the “internal operations” exception. The COPPA statute gives broad authority to the Commission to promulgate regulations governing the collection of personal information, including the scope of the “internal operations” exception.⁷⁶ However, the Commission should not follow the proposal put forward by some commenters to exclude personalization based on whether it is “user-driven.”⁷⁷ As the Commission recognizes, the term “user-driven” is unclear,⁷⁸ especially given that much personalization is driven by the user’s previous actions, such as the user’s posts or interactions with other users.⁷⁹ In that sense, much personalization online is “user-driven.”

Instead, the Commission should focus on whether the personalization is based on a profile of the user. Although “profile” is already used in the current Rule, the Commission may define a “profile” as “information identifying a child’s online activities over time, whether across an operator’s own websites or online services or third party websites or online services.”⁸⁰ This approach would be more administrable and would focus the Rule on its

⁷² NPRM at 2070–71.

⁷³ *E.g.*, *Social and the Teen Mental Health Crisis: Hearing Before the Sub-Committee on Consumer Protection, Product Safety, and Data Security* (Nov. 7, 2023) (statement of Arturo Bejar), [here](#); *Protecting Kids Online: Hearing Before the Sub-Committee on Consumer Protection, Product Safety, and Data Security* (Oct. 5, 2021) (statement of Frances Haugen), [here](#).

⁷⁴ Letter from Cody Venzke, American Civil Liberties Union, to Sen. Maria Cantwell et al. (July 27, 2023), [here](#).

⁷⁵ Brief of Amici Curiae of the American Civil Liberties Union, American Civil Liberties Union of Arkansas, & Electronic Frontier Foundation at 17, *NetChoice LLC v. Griffin*, No. 23-cv-5105, ECF No. 31 (July 24, 2023), [here](#) (“Age verification requirements are more restrictive than policies enabling or encouraging users (or their parents) to control their own access to information”); *accord* *Ashcroft v. ACLU*, 542 U.S. 656 (2004) (device-based filters less restrictive than age verification); *Rowan v. U.S. Post Off. Dep’t*, 397 U.S. 728, 733 (1970) (upholding statute allowing individuals to bar mail from particular senders, as it granted “the addressee complete and unfettered discretion in electing whether or not he desired to receive further material from a particular sender” and did not implicate state action).

⁷⁶ 78 Fed. Reg. 3972, 3980 (Jan. 17, 2013) (citing the Commission’s authority to define scope of “personal information”).

⁷⁷ NPRM at 2070.

⁷⁸ *Id.*

⁷⁹ Adam Mosseri, *Instagram Ranking Explained*, Instagram (May 31, 2023), [here](#).

⁸⁰ American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 2(28)(A)(xv) (2022).



core purpose: giving parents and children control over the use of their personal information.

Regarding push notifications, the Commission should carefully consider whether a categorical exception is permitted by the statute, or if more robust guidance and enforcement is more appropriate. The statute states that the Rule “shall” permit operators to respond “more than once directly to a specific request from the child,” so long as parents are provided notice and an opportunity to opt-out.⁸¹ The statutory language is mandatory and does not provide for exceptions for use cases such as push notifications, so long as the operator meets the notice and opt-out requirement. Consequently, it is not clear that the Commission has authority under the statute to amend the Rule for a specific type of repeat contacts such as push notifications or prompts.

However, the statute *does* require that the notice be in response to a “specific request” from the child; it also limits subsequent responses to the “scope of that request.”⁸² There may be many instances where push notifications do not meet those requirements, suggesting more proactive enforcement by the Commission may be more appropriate than amending the Rule.

Conclusion

The ACLU thanks the Commission for its continued focus on privacy not just for children but for all people. Control over our personal information is increasingly central both to controlling our online experiences and to preventing misuse of that information. If the Commission has any questions about these comments, please do not hesitate to contact us at cvenzke@aclu.org.

Sincerely,

Chris Anders
Director, Democracy & Technology Division
National Political Advocacy Department
ACLU

Cody Venzke
Senior Policy Counsel

⁸¹ 15 U.S.C. § 6502(b)(2)(C).

⁸² *Id.*