

March 11, 2024

Via <https://www.regulations.gov>

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

COPPA Rule Review, Project No. P195404

Privacy Vaults Online, Inc. ("PRIVO"), over the past twenty years, has become one of the leading global industry experts in minors' online privacy, identity, and consent management. PRIVO has served as an FTC-approved COPPA Safe Harbor since 2004 and has participated extensively in all Commission proceedings addressing COPPA and in Safe Harbor roundtables, lending its extensive experience to help inform the Commission and industry on issues of children's privacy and developments in the marketplace affecting it.

Our comments reflect our experience over the years actively engaging in consulting with corporations and organizations, many struggling to interpret COPPA and developing and employing a privacy compliant technology solution to obtain verifiable parental consent and age verification. The company's leadership has invested time and attention to deeply understand the operational challenges introduced by minors' privacy compliance requirements in the United States and globally. We take great pride in the role we play in ensuring children's privacy and we look forward to collaborating with all efforts to improve success across the entire ecosystem of protection for minors.

PRIVO offers comments on the various issues raised in the Federal Register Notice:

A Definitions

1. Online Contact Information

To improve the Rule's functionality, the Commission proposes amending this definition by adding "an identifier such as a mobile telephone number provided the operator uses it only to send a text message" to the non-exhaustive list of identifiers that constitute "online contact information."

In keeping with the intent of COPPA, it is a core value to PRIVO that parents be given freedom and flexibility with respect to how they wish to complete the parental consent process so that

they can most effectively make use of the rights they are granted under COPPA and actively participate in the protection of their children’s online privacy. For this reason, PRIVO has commented in numerous proceedings before the Commission warning against any efforts that might force parents through a one-size-fits-all verification process in the name of reducing friction for operators, but not necessarily for parents. Consistent with that, PRIVO is appreciative of the effort to modernize the definition of “online contact information” to include mobile telephone numbers. However, it bears noting that a mobile phone number is more than simply today’s version of the e-mail address envisioned at the time of COPPA’s passage. There are a number of special considerations that arise with the collection and use of mobile phone numbers, especially from a minor, and require further analysis and guidance from the Commission.

One concern is the issue of consent. The Commission should address whether a child can consent on behalf of the parent to the receipt of a text message by the parent. Various state and federal laws require the prior express consent of the recipient to receive various types of text messages, including marketing messages.¹ In numerous class action lawsuits across the country, consent given by a third party has been challenged.² Moreover, even if third-party consent is appropriate, there is the issue of the age of the party giving consent under state laws.³ In addition, to make the text messages useful to parents who receive them unexpectedly (since they are not the ones triggering the sending of the texts), the messages must contain a considerable amount of information identifying the sender, the purpose of the text, information already collected from the child, the consent being requested and a link to the additional required COPPA disclosures. Such contents, particularly links to commercial websites, have given rise in the past to arguments that the texts contain marketing content as well as informational content, giving rise to additional restrictions and potential litigation.⁴

Another concern is with the amount of personal data that attaches to consumers’ mobile telephone numbers, including name, address, and much more, while none of that may be

¹ See, e.g., Telephone Consumer Protection Act, 47 U.S.C. § 227 et seq.; National Do-Not-Call Registry 15 U.S.C. § 6151; Oklahoma Telephone Solicitation Act of 2022, 15 OK Stat § 775C.1.

² See, e.g., *Hall v. Smosh Dot Com*, 72 4th 983 (9th Cir. 2023). See also *In the Matter of Cargo Airlines Association Petition for Emergency Declaratory Ruling*, Order, 29 FCC Rcd 3432, ¶ 10 (FCC 2015), 89 FR 15688 (Mar 25, 2015) (FCC declining to clarify that package shipping companies can rely on consent received from package senders to text delivery notifications to their package recipients).

³ A similar question arises as to whether operators can rely on consent given by children under the age of 13 to send the children text messages at the mobile telephone number they represent to be “theirs,” given state laws that set the age of majority at the age of 18 or even older, and the terms of service applicable to various mobile phone plans usually subscribed to by someone other than the child purportedly giving the consent.

⁴ Texts sent pursuant to Section 312.5(c)(2), where parental consent is not required, but the operator only seeks to voluntarily update the parent about the child’s participation with the online site or service could be particularly problematic as they are neither solicited by the parent nor sent for any purpose arguably required by COPPA.

associated to any particular email address a parent has. In PRIVO's experience, parents typically have numerous email accounts, such as one for work, one for friends and family, one for online shopping, one for social media accounts, and one for kids' school and activities. In contrast, parents tend to have only one mobile telephone number. This makes sense in that email accounts are readily available for free and easy to set up while mobile phone accounts are not free but are easily ported with the consumer from carrier to carrier throughout their lifetime. Mobile phone numbers are collected in connection with many consumer transactions, from online banking transactions to registering for online and brick and mortar retailers' loyalty programs. As a result, the amount of data available to data brokers to create profiles of consumers and their purchasing habits based on having their mobile telephone number is vast and potentially much greater than that available to them via an email address. Consideration should be given to whether parents' participation in the required parental consent process, triggered by the child and not the parent him or herself, unnecessarily exposes parents to the potential for increased data mining.⁵

Finally, there are issues of a more procedural nature to be considered. For example, where the sender of the text message is identified merely by a five-digit number or an unfamiliar telephone number, parents may not recognize the sender. Upon initial receipt of the text message, the inability to recognize the sender may lead the parent to not take the steps necessary to permission their child as requested, which undermines the method's initial effectiveness. However, if the parent does permission the child as requested, the inability to easily identify the sender could still be an issue, later, when the parent attempts to withdraw consent or asks to review the data the operator has collected on the child. Parents may be hindered in their ability to exercise these rights to the extent they cannot find the original text message to return to it, review the disclosures, and contact the operator. Another potential issue arises with the parent who, not recognizing or expecting the text message, engages in normal texting behavior and responds STOP to it. This response may not provide a clear answer as to whether the parent has declined to permission the child's use of the site or service or simply asked to not be contacted by text. If the operator deletes the child's and parent's information because the parent has not responded, it will not have the information needed to honor the STOP request, should the child seek parental consent a second, or third, or fourth time. Finally, it should be remembered that obtaining consent via text message will not be limited to a single text message. If the parent does not respond within a reasonable period of time, it is likely they will receive one or more reminder text messages. In addition, if the operator updates its Privacy Policy, or the child activates a feature of the site or service that requires a higher level of parental verification, additional text messages will have to be sent unless other contact information is also secured from the parent. If the proposal in this

⁵ In this regard, it is noted that standing up a free-to-end-user texting program for the management of parental consent can involve significant costs. Operators may thus be incentivized to utilize free texting programs that might capture parent and child data and utilize it in non-COPPA compliant ways.

proceeding to require additional consent before disclosure of child data is adopted, the number of text messages could be much higher. There is a risk that these text messages, especially from multiple children seeking access to multiple sites and services, will be much more intrusive on parents, especially those who bring their own devices to work or leave them next to their beds at night, than the e-mail method would be.

For all these reasons, if the definition of online contact information is amended to include mobile telephone numbers, additional guidance will also be needed. To be clear, collection of mobile telephone numbers can be effectuated today, observing the existing COPPA requirements. Any changes should be made only after careful consideration of the multiple issues involved and of the potential for operators to rely on a Commission rule allowing texting without a full appreciation of the other regulatory requirements surrounding it.

2. Personal Information

a. Biometric Data

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

PRIVO agrees with the expansion of the Rule’s coverage to include biometric data. Children are a vulnerable section of society. This data captured from a child will create a profile of them for a lifetime and could result in decision making that will have an effect on their lives. Such sensitive data should only be required when needed for a specific purpose and secondary use should be prohibited.

3. School and School-Authorized Education Purpose

As discussed in Part IV.C.3.a., the Commission proposes codifying current guidance on ed tech by adding an exception for parental consent in certain, limited situations in which a school authorizes an operator to collect personal information from a child. The Commission also proposes adding definitions for “school” and “school-authorized education purpose,” terms that are incorporated into the functioning of the proposed exception and necessary to cabin its scope.

PRIVO believes that codifying the FTC’s guidance on School and School Authorized Education Purpose can help prevent the widespread practice of individuals claiming a role of teacher, consenting to the collection and use of children’s personal data without the required protections in place. Flexibility should be included to allow the child, with parental consent, to

transition the account for use outside of school, for example, to continue developing skills over the summer or when transitioning to homeschooling or between schools.

C. Parental Consent

1. General Requirements

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

PRIVO believes that where a feature such as disclosure is not integral to the use of the site or service, notice and parental verification/consent should occur at the time access to the feature is sought. For example, if the parent does not consent to non-integral disclosure, then parental verification can occur at a lower level on the sliding scale. If access to that feature is sought at a later time and the parent wishes to permission its use, a new verification at the higher required level should then occur. While the consent should be granular to the features of the site or service, notice and parental verification/consent need not be separated.

2. Methods for Verifiable Parental Consent

The Commission also agrees with the recommendation that it modify the Rule to eliminate the monetary transaction requirement when an operator obtains consent through a parent's use of a credit card, debit card, or an online payment system.

The Commission would also welcome information on the role that platforms could play in facilitating the obtaining of parental consent.

PRIVO opposes eliminating the monetary transaction requirement for obtaining full verifiable parent consent. This is a step backwards as it allows permissioning at the highest level of assurance without any transparency to the parent or accountability by the service. In PRIVO's experience, when the credit card method is offered, up to 11% of the time, parents will use it when they know that the charge will be refunded. Therefore, cost to the parent should not be held up as a reason to not offer credit card as one of multiple methods for the parent to verify themselves. Indeed, PRIVO notes that, increasingly, debit cards (as well as gift cards) are available to and used by children under 13. Accordingly, PRIVO would request that the Commission revisit the approval of debit card as an approved method and disallow it.

With respect to the role that platforms might be able to play in parental consent management, PRIVO notes that the Commission has already approved information and consent intermediaries, "infomediaries," when it approved PRIVO's Safe Harbor application in 2004. So,

there is no legal impediment to platforms such as app stores being able to take on an active role. However, the user's desire to access the site or service from multiple platforms – laptop, Android, iOS, sideload app – creates logistical challenges for the management of conflicting consents to features and functionalities across multiple platforms. The additional data that such platforms could acquire as managers of granular consent preferences and choices throughout a lifetime also has the potential to create an overly-rich profile informed by information about children's preferences and desires and what their parents will allow them to participate in.

As to new methods, PRIVO reiterates its prior comments that Commission should encourage smarter age gates. Current age gates are too easily defeated by children clearing cookies and offloading and reloading apps. Age gates should have more persistent blocks to prevent the same.

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

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

PRIVO supports strengthening data security and integrity and believes that proportionality to the amount data processed and retained is important. PRIVO already requires this for its members.

G. Data Retention and Deletion Requirements

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

PRIVO has long supported and implemented such a requirement.

H. Safe Harbor

1. Criteria for Approval of Self-Regulatory Program Guidelines

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

2. Reporting and Recordkeeping Requirements

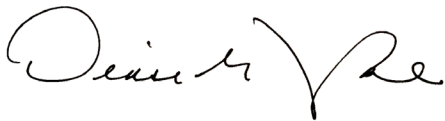
The Commission proposes to require FTC-approved COPPA Safe Harbor programs to identify each subject operator and all approved websites or online services in the program, as well as all subject operators that have left the program.

PRIVO records, maintains and publishes each operator and its approved services publicly and in its annual report to the FTC and welcomes the inclusion of such requirements to ensure all safe harbors meet the requirement.

The Commission proposes to add a requirement that FTC approved COPPA Safe Harbor programs submit a report every three years outlining its technology and mechanisms for assessing subject operators' fitness for maintaining membership.

This requirement is welcomed. Safe harbors should provide a robust and comprehensive program that meets or exceeds requirements. The tools required to do so are integral to running such a program. Safe harbors that fail to run robust programs undermine the self-regulatory framework that provides an essential tool in the box that supports companies and the FTC to build a privacy safe online environment for younger children.

Sincerely,



Denise G. Tayloe
Co-Founder & CEO
PRIVO



Claire Quinn
Chief Privacy Officer
PRIVO