INTERNET
SAFETY
//LABS

March 11, 2024

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Washington, DC 20580

Subject: Re: COPPA Rule Review, Project No. P195404, Docket ID FTC-2024-0003

Internet Safety Labs (ISL) is pleased to provide comments on the COPPA rule updates from the FTC and the proposed questions. Regulation such as COPPA must be regularly updated to keep pace with speed of technological change, and ISL commends the FTC's efforts in this undertaking.

Detailed Responses to Questions:

General Questions

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

Regarding the proposal to require operators to provide access to all school agreements: ISL agrees that the publication of school agreements is crucial for parental and student awareness. ISL suggests that the FTC work with the USDE to make a similar requirement for schools/LEAs to publish data privacy agreements for all vendors. The Student Data Privacy Consortium provides an excellent platform to facilitate this, but even just a posted spreadsheet with links to the agreements on the school or district's website would be adequate. Schools should be maintaining this list as a matter of vendor management practice.

In our research, schools in the US recommend or require 20 technologies on average (2022 K-12 EdTech Benchmark Findings Report 2: Demographic Analysis of App Safety, Website Safety, and School Technology Behaviors in US K-12 Schools, February 6, 2024). Imagine as a parent having to go to 20 or more different operator sites, search for your school's agreement, read it, possibly

save it and file it. It would be much easier and practical for both parents and students to have a simple, single list from their school.

See also the Tableau dashboard for sampling data:
https://public.tableau.com/app/profile/internetsafetylabs/viz/K-12EdTechBenchmark2022/StateSummary

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

There's no way such automated means will work – the only way to reliably delete PII from communication is to delete the communication. There are too many subtle ways that small details can reveal information.

Additionally, there is potential for any deletion mechanism, even a total one, to have bugs which result in information leakage or misuse. The rules should be simple to make enforcement as easy as possible, given the extreme difficulty of monitoring what operators do with data on their own servers.

ISL also believes that "publicly available" is too permissive a test. Operators should be forbidden to publicize personal information of children, even if the set of parties to whom they publicize it is not the entire world.

ISL further notes that any deletion requirement that is to be meaningful needs to specify particular timelines within which deletion must occur. Operators are incentivized to retain data as long as permissible; the Commission should specify and enforce specific upper bounds rather than allowing companies to decide for themselves.

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?

Of course it's a risk, it encourages phishing. It is inappropriate to bombard parents with requests for permission through spoofable channels such as text messages and email, as it leads them into the habit of always authorizing requests without carefully vetting that they are genuinely from an operator and not an impersonator.

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 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?

Yes.

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?

The most important thing to consider with regard to any user identifier is that resettable identifiers are safer than non-resettable ones in regard to unwanted contact, because in principle if a user can change their identifier to a new one, they can mitigate the harm more easily. However, with usernames there is a tension because, even when the option exists to reset it, people are emotionally attached to the name and don't want to change it.

One technique some services employ is to split the username into a human-readable part and a number. These services then allow either part to be changed, any number of times. This allows people who are the recipients of unwanted

contact to "move" to a new identity without giving up the name they may have an attachment to.

An alternate approach, which has been used in particular with audiences of younger children, is to make these identifiers entirely opaque and not meant to be memorized by humans – for example, making them large random numbers. It is still important that these be resettable; the benefit of making them opaque is that users are more willing to reset them.

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?

Keep the rule.

Add "typing cadence" to the list of biometric identifiers.

Do not allow a deletion exception, it's all but impossible for external oversight to verify that deletion has actually occurred. Operators of identity verification services are strongly incentivized to retain data for the sake of their business model. Additionally, there are emerging risks involving the training of ML models with the use of personal information as training data, which is currently a complex legal area that risks allowing operators to escape accountability for improper retention of data despite the harms being real.

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?

Avatar images, whether generated from a child's image or not, definitely need to be treated as PII. Avatars can be used by stalkers due to the tendency to reuse them – like usernames.

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?

No response.

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?

Add "guardian(s)" in addition to "parents". Also consider adding "family members".

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

No response.

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?

Yes, the Commission should consider changes to the provision allowing persistent identifiers for contextual advertising. ISL contends that advertising related persistent identifiers for children are unacceptable under all circumstances. These identifiers enable data brokers and others to create data profiles which can be sold as well as used for deliberate manipulation. Current digital advertising (and realtime bidding) results in the "largest ongoing data leak"[1]. Until Realtime Bidding (RTB) and adtech infrastructure can be done in a way that doesn't leak data, it must be removed from all child-directed sites and services. ISL recognizes this position may seem extreme and that people will say that removing "free" services for children harms them. ISL is confident in the creativity of technologists to develop a safer form of digital advertising that doesn't rely upon or enable uniquely identifying children and facilitating the profiling of children. There is of course historical precedent in protecting the developing and impressionable minds of children from influence/manipulation by advertising.

[1] Lomas"Adtech 'data breach' GDPR complaint is headed to court in EU", Natasha Loma, June 16, 2021. Techcrunch. https://techcrunch.com/2021/06/16/adtech-data-breach-gdpr-complaint-is-headed-to-court-in-eu/

The proposed usage restriction of a persistent identifier is likely inadequate, namely, restricting use of a persistent identify "to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose". ISL recommends striking the word "behavioral" from the list of restricted usage.

Furthermore, usage restrictions are quite difficult to enforce in the advertising ecosystem because information typically passes through the hands of multiple parties who do not audit each other.

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?

In an ideal world, operators should require no incentive to continually assess the likelihood of child users of their services.

Regarding this from the rule-making document:

> **"**Through the 2013 Amendments, the Commission intended mixed audience sites and services to be a subset of the "child-directed" category of websites or online services to which COPPA applies."

ISL finds the characterization of mixed audience sites as a "subset of the 'child-directed' category of websites or online services to which COPPA applies" confusing, and that, in practice, mixed audience sites are a subset of *all* sites, not just child-directed sites.

In our research (2022 K-12 EdTech Safety Benchmark: National Findings – Part 1, 12/13/22), 28% of all technologies recommended by K-12 schools for students is *not* for children. There are no sovereign boundaries on the internet, and it will always be the case that children will explore and use technology not intended for children—sometimes at the recommendation or requirement of schools or teachers. So, either an operator makes their service COPPA compliant for *all* users, or they must provide COPPA protections for users under the age of 13.

Moreover, if a service doesn't have a minimum age requirement, it should be assumed to have a mixed audience and act accordingly.

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?

No response.

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?

ISL recommends that the language "collect age information" must be avoided/removed as it implies an implementation detail, namely, that a site *collect*—which seems to also imply retention of—age information. This behavior is *not* required to achieve the goal. Rather, the language should focus on "age verification", which suggest a more "forgetful" implementation, where the site/service can either use a verifiable credential, or confirm age via some other means and then *only* retain a boolean of "user under age 13: Y/N", thus the service need not retain age information.

(https://www.w3.org/TR/vc-data-model/, new version in progress: https://www.w3.org/TR/vc-data-model-2.0/)

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?

ISL believes it is NOT acceptable for any percentage of children as an audience to be excluded from COPPA protections. Incentivizing surveillance of *all* users must be avoided.

d. 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?

Since "competent and reliable empirical evidence regarding audience composition" is already included as a factor, the FTC should clarify and strengthen what constitutes competent and reliable empirical evidence, including use of machine learning. For instance, ISL is augmenting our Safety Labels (https://appmicroscope.org) with the number of Elementary and Middle schools found to be actively recommending or requiring the technology to its students. This kind of data from school/district websites should be considered as "competent and reliable empirical evidence regarding audience composition".

ISL also notes that the current guidelines for "actual knowledge" incentivize operator ignorance in a digital world rife with commercial surveillance. ISL recommends greater clarity and additional criteria/scenarios for supporting actual knowledge.

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)?

Why is this an either/or and not a "both"? It must be included in the direct notice under section 312.4(c) for the parent to provide initial consent. This notice is likely to be processed by the parent at the time of provisioning the service for the child. Whereas the notice in 312.4(d) is likely to be accessed while the service is used. Thus, if the third-party sharing behavior changes, it is more likely to be observed/noticed in the online notice. (Unless operators were required to send updates to the parents any time the list of third-parties changes. ISL recognizes the drawbacks of this kind of notification; it could be information overload resulting in all such notices becoming "noise", and being ignored. We are precariously close to this kind of inured apathy towards online notices in general.)

Parental Consent

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

    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?

ISL believes consumers deserve to know *all* the invisible third-party sharing behaviors of the technology, whether it is "integral" or not. Further, ISL believes parents should have the right to consent to all third-party sharing, whether it is deemed integral or not.

ISL further questions why technology used by children is sharing a child's personal information with a third party that is not "integral" to the expected service. The characterization of "integral" vs. "non-integral" is possibly too crude a taxonomization, as well as being easy for operators to manipulate. Perhaps COPPA should consider adopting the GDPR's six legal bases for data processing as a way to clarify PII usage. In any case, even if the purposes were further taxonomized, ISL remains firm that consumers have a right to know who the data's being shared with and for what purpose—this is even more important for children. Note that ISL provides a tool to expose these third parties in our app Safety Labels viewable via https://appmicroscope.org

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

(1) While there are no existing norms/recommendations for precisely how to minimize addictive design, the FTC should develop [with a multidisciplinary team of experts and concerned users of technology] guidelines for minimally addictive technology practices for child-directed services. This should include guidance regarding the use of online rewards and "like" buttons, and use of infinite scroll, for example.
(2) Personalization must be opt-in, only. Technology must be impersonal by default.
(3) Engagement techniques must not be used to drive children to financialized experiences. For example, to the extent that operators' services include functionality which invites children to create content for financial gain; to speculate on the value of content; to promote content in which they have a financial interest; or to utilize currency-like features, whether readily exchangeable with fiat currency or otherwise, engagement techniques must not be used to repeatedly nudge children towards engaging with such features.

So long as online "engagement" means a strategy for revenue generation, extra care must be taken for child users of technology.

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

ISL appreciates the alignment of COPPA with FERPA, but there are some issues:

(1) Per the document:

"As an extra safeguard to help ensure that ed tech providers are using student data appropriately and to align the exception with FERPA, the required written agreement must specify that the school will have direct control over the provider's use, disclosure, and maintenance of the personal information under the exception."

This is a reasonable aspiration/intention but schools ultimately have little control over the operator's use, disclosure and maintenance of the student information under the exception. With the proposed new notice, schools will have crucial information about what the operator says they're doing with the data, but ISL believes that the definitive "knowability" of the sharing of data is not 100%—especially with any kind of digital advertising in the service.

Regarding the scope of "school-authorized education purpose", one option is for COPPA to align closely with FERPA allowed exceptions, which is broader than "education" purposes, strictly speaking.

ISL also recommends that schools must allow parental consent when any of the protected information per PPRA is processed (i.e. collected or shared). This includes political affiliation, mental health, sex behavior and attitudes, religion, etc.

In our research (2022 K-12 EdTech Benchmark Findings Report 2: School Technology Practices & 3rd Party Certifications Analysis, June 27, 2023), we found evidence of a serious problem of schools/districts over-applying their ability to consent on behalf of parents. This site from Norfolk Public Schools in Virgina, for example lists 754 sites for which the school is consenting, many of which sites don't require accounts for usage; it's clear that the school has no relationship with the majority of these services. This was seen in several schools.

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

Information

17. COPPA and § 312.7 of the Rule prohibit operators from conditioning a child's participation in an activity on disclosing more personal information than is reasonably necessary to participate in such activity.
    a. What efforts are operators taking to comply with § 312.7? Are these efforts taken on a website-wide or online service-wide basis, or are operators imposing efforts on a more granular level?
    b. Should the Commission specify whether disclosures for particular purposes are reasonably necessary or not reasonably necessary in a particular context? If so, for which purposes and in which contexts?
    c. Given that operators must provide notice and seek verifiable parental consent before collecting personal information, to what extent should the Commission consider the information practices disclosed to the parent in assessing whether information collection is reasonably necessary?

No response.

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"?

No response.

Safe Harbor

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

1. There is a natural conflict for Safe Harbor certifiers who are incentivized by increasing the number and type of platforms that they certify. Certification programs in general are motivated towards passing application.

2. ISL questions whether some technologies *can* be certified. For instance, advertising platforms [supply side platforms (SSPs)] are currently certified by some Safe Harbor programs. Certifying ad platforms is tricky due to the configurability of these platforms. ISL has an active responsible disclosure in progress and will soon be publishing details of such a COPPA certified ad platform being mis-configured by the publisher, resulting in use of the non-COPPA compliant advertising functionality.

To provide more details, ISL has found confusion around the responsibility and configuration of Ads.txt files. These files are managed by a domain manager (in this case, the domain manager is the SSP), but the file is ultimately the responsibility of the publisher. So while the SSP has been COPPA Safe Harbor certified, the site publisher is using the non-COPPA specific ads.txt file.

3. ISL believes that COPPA Safe Harbor certifiers need to perform more investigation of the actual technology behavior. For instance, apps in our 2022 US K-12 EdTech Benchmark Findings Report 2, ISL found that, while COPPA Safe Harbor certification was effective at removing behavioral ads, certified apps had more digital advertising than the overall population of apps. 26.2% of COPPA Safe Harbor certified apps included digital ads, compared to 17.6% of the total sample of over 1700 apps.

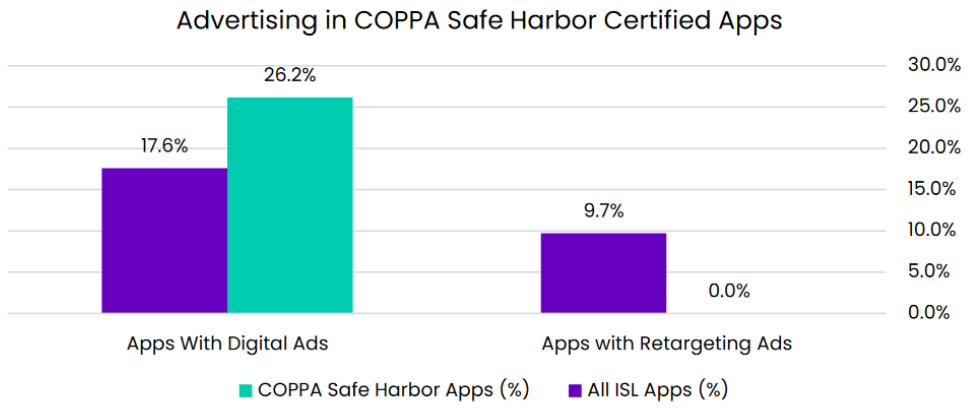
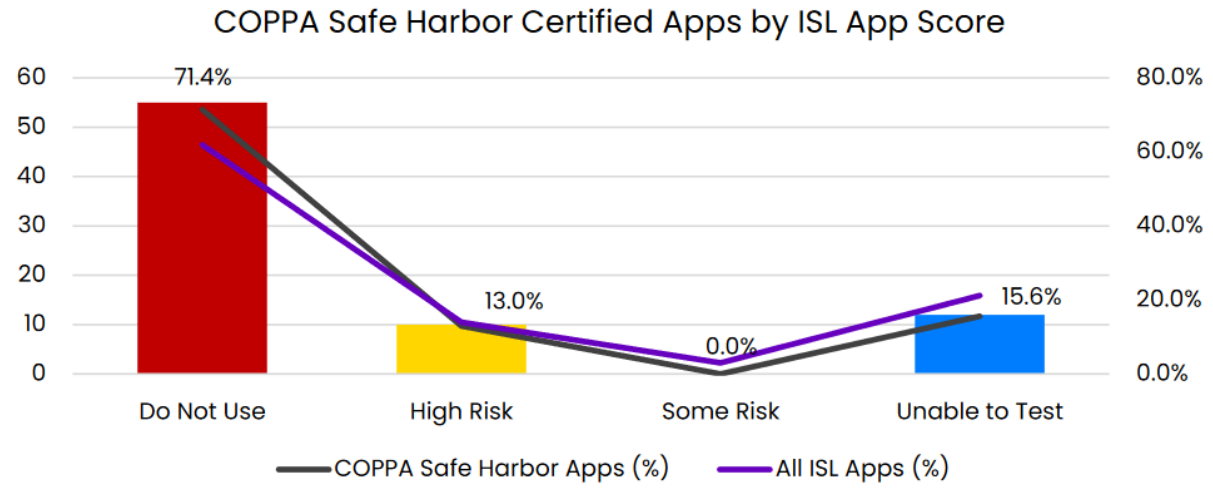


Figure 7.9a

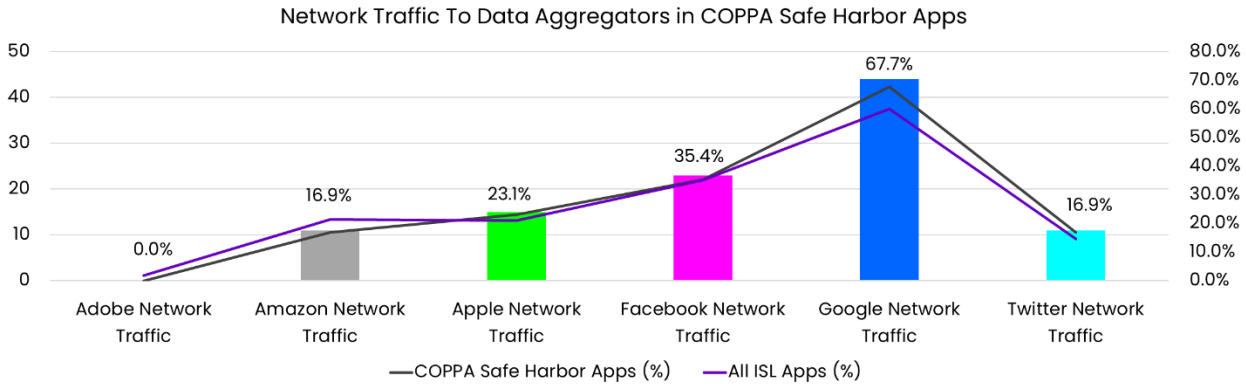
Source: "2022 K-12 EdTech Benchmark Findings Report 2: School Technology Practices & 3rd Party Certifications Analysis" pg 74. Internet Safety Labs. June 27, 2023.

COPPA certified apps also were more likely to receive our highest risk score than the overall set of apps:



Source: "2022 K-12 EdTech Benchmark Findings Report 2: School Technology Practices & 3rd Party Certifications Analysis" pg 63. Internet Safety Labs. June 27, 2023.

The chart below shows the percentage of COPPA Safe Harbor certified apps sending data to aggregator platforms.



Effective Date

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

No response.