Children's Advertising Review Unit (CARU)®
Of BBB National Programs, Inc.

Submitted Electronically
December 11, 2019

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

RE: ***COPPA Rule Review 16 C.F.R. Part 312, Project No. P195404***

Dear Acting Secretary Tabor:

The Children's Advertising Review Unit (CARU) of BBB National Programs, Inc. (BBB NP)[1] is pleased to have an opportunity to comment on the above-referenced COPPA Rule Review.

CARU was founded in 1974 as the self-regulatory arm of the children's advertising industry. Since its inception, CARU has been tasked with protecting children from deceptive or inappropriate advertising in all media by working with companies to ensure that their advertising complies with CARU's self-regulatory guidelines (as well as any applicable laws). In 1996, before COPPA was legislated, CARU was at the forefront of safeguarding children's privacy by updating its guidelines to address children's privacy. It was these guidelines that helped create the foundation of COPPA.

CARU offers comments on the following questions raised in the Federal Register notice: General Questions for Comment, Sections (B) Definitions, 12-15: (H) Confidential, Security and Integrity of Personal Information, 28 and; (I) Safe Harbors, 29.

12. The 2013 revised COPPA Rule amended the definition of "Personal information" to include, among other items, a "persistent identifier that can be used to recognize a user over time and across different websites or online services." Has this revision resulted in stronger privacy protection for children? Has it had any negative consequences?

The addition of "persistent identifier" to the definition of "Personal Information" has resulted in improved privacy protections for children but has had some negative consequences for industry, specifically the lack of robust and creative child-directed content.

In its experience as a COPPA Safe Harbor provider and self-regulator, CARU has had the opportunity to work with many operators of online services for children, both small organizations and large ones. The addition of persistent identifier to the definition of personal information has resulted in improved privacy protections for children because operators are more aware of what information they are passively collecting from children. It also created clear rules prohibiting the practice of interest-based advertising

[1] BBB National Programs, Inc. (BBB NP) administers independent self-regulatory and dispute resolution programs including CARU, BBB EU Privacy Shield, Digital Advertising Accountability Program and the National Advertising Division. BBB NP is a mission-driven non-profit with programs funded by businesses and associations that share our mission in promoting trust in the marketplace.

and amassing profiles of children's behavior online without first obtaining verifiable parental consent. The difficulty with the overall compliance for this provision is wide-spread confusion about what is included in the definition of "support for internal operations," including the meaning of "for any other purpose" in section 312.2(2), as it applies to the exception to prior parental consent in section 312.5(7) of the Rule.

Most operators understand how to ensure that their products do not collect and use data for the purpose of interest-based advertising or to track their users over time and across platforms. However, in CARU's work with companies in its safe harbor program, explaining why they cannot collect a persistent identifier "for any other purpose" has been challenging. CARU asks that the FTC provide clarification and/or examples of instances that would be deemed "for any other purpose." As technology evolves, the online ecosystem of services and service providers that are available to operators is continuously expanding. Many of these services engage in the business of behavioral advertising but also provide services that could legitimately fall within the scope of the "support for internal operations" exception, including for analytics and contextual advertising.

Without a full understanding of what is proscribed and why, operators - especially smaller companies - struggle with how to ensure that their third-party vendors and service providers are using the information provided to them in a COPPA-compliant manner. Furthermore, operators have difficulty ascertaining whether a third party is respecting a child-directed flag and only collecting persistent identifiers for specific purposes. Since liability for the first party operator is absolute, individual agreements with providers are necessary, but executing these for multiple products can be prohibitively costly for companies and result in a chilling effect on the creative content and number of compliant products available to children.

Recently, the leading mobile app platforms have tried to limit the collection of Personally Identifiable Information (PII) by third parties for apps in the kids and family categories. These new requirements either prohibit operators from sharing PII with ad networks altogether or require them to self-certify as COPPA-compliant.[2] Other requirements restrict operators from using third-party analytics providers that collect or transmit the identifier for advertisers (IDFA) or any identifiable information about children (such as name, date of birth, email address), their location, or their devices.[3] While this is helpful from a privacy perspective, it may result in fewer operators wanting to include their apps in the kids and family categories[4] thus resulting in fewer protections for children and less help to parents who struggle to understand what products are safe for children.

---

[2] See Google Play Guides for Creating Apps and Games for Children and Families at: https://developer.android.com/google-play/guides/families

[3] See Apple App Store Review Guidelines at: https://developer.apple.com/app-store/review/guidelines/#1.3. Apple delayed enforcing these new guidelines for the time being. For details see, https://www.washingtonpost.com/technology/2019/08/20/apple-aims-protect-kids-privacy-app-makers-say-it-could-devastate-their-businesses/

[4] This is especially likely for apps produced by foreign operators, who are less likely to be held accountable for COPPA compliance.

CARU believes that service providers in the online ecosystem need to provide more transparency on their child-directed services. CARU has observed that most service providers do not state in their privacy policies or terms of service whether their service is appropriate for an online service directed to children, i.e. COPPA compliant .[5] At the conclusion of the last COPPA Rule review in 2013, CARU encountered a handful of service providers doing one of two things: clearly stating their service should not be used with online services directed to children or; creating a COPPA-compliant version of their service. Unfortunately, there has not been a proliferation in the marketplace of the latter.

CARU recommends that the Commission provide additional guidance of what "for any other purpose" includes and how the collection and use of such information can negatively impact the privacy of children. A better understanding of this definition will allow operators to negotiate more efficiently and economically with third-party vendors to comply with the Rule and promote an overall privacy-by-design philosophy.[6] CARU also recommends that service providers present a clear explanation in their privacy policies of how their service can be used in a manner that complies with COPPA or specify that their service cannot be used by online services directed to children.

13. Should the Commission consider further revision to the definition of "Personal information"? Are there additional categories of information that should be expressly included in this definition, such as genetic data, fingerprints, retinal patterns, or other biometric data?

In 2013 the COPPA Rule was modified to expand the definition of personal information to include persistent identifiers, geolocation information, photos, videos and audio recordings. The stated reason for this change was to modify the definition "in light of changes in online technology since the Rule went into effect in April 2000."[7]

The underlying intent of COPPA is to provide parents with greater control over their children's personal information. And the law has rightly evolved with technology to protect children's data such as photos and audio recordings.

The collection and use of biometric data, (e.g. fingerprints, retinal scans, facial recognition, etc.) in the tech industry has exploded in the last decade. It is now commonplace for individuals to unlock their mobile phones using fingerprint or facial recognition. Recent studies have shown that[8] many of the

[5] Most service providers state in their privacy policies that they do not knowingly collect the personal information of users under 13.
[6] CARU recommends clarification, if not in the COPPA Rule, then in the FTC guidance, "Complying with COPPA: Frequently Asked Questions" at: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.
[7] 16 C.F.R. 312.2, 78 Fed. Reg. No. 12 at 3972 (Jan. 17, 2013).
[8] Rideout, V., and Robb, M. B. (2019). The Common Sense census: Media use by tweens and teens, 2019. San Francisco, CA: Common Sense Media. See: https://www.commonsensemedia.org/sites/default/files/uploads/research/2019-census-8-to-18-full-report-updated.pdf

people using these phones are children under the age of 13. Although the use of biometric data has become commonplace, only three states currently provide legal protections regarding biometric data, (Illinois, Washington and Texas) and there is no applicable federal law. The collection of biometric data presents far-reaching and serious risks to privacy as it is specific to each individual, unalterable and is permanent.[9]

In recognition of these risks, the Illinois legislature passed the Biometric Information Privacy Act (BIPA) in 2008 to regulate businesses that use biometric data. The purpose of the Act was to establish standards of conduct for private entities that collect or possess biometric information. BIPA defines "Biometric identifier" as… "**a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.** [Emphasis added]."[10] BIPA defines "Biometric information" as any information, regardless of how it is captured, converted, stored, or shared, **based on an individual's biometric identifier used to identify an individual. [11][**Emphasis Added]

The policy considerations underlying COPPA and BIPA were similar in sharing the goal of protecting individual citizen's privacy and recognizing that the collection and use of certain sensitive information requires a heightened level of consent. COPPA defines personal information as "individually identifiable information about an individual collected online."[12] COPPA's current definition of "personal information" is broad enough to give the FTC the authority to include biometric data.

While BIPA protects individuals in Illinois there is no federal protection on this front, nor does the Illinois law carve out special provisions for children as is COPPA's over-arching purpose. Whereas COPPA requires that verifiable consent[13] must come from a parent or guardian, BIPA construes consent more broadly and does not specifically refer to an age of consent.[14]

---

[9] Gartland, Claire. "Biometrics are a Grave Threat to Privacy" New York Times, July 5, 2016. See https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-are-a-grave-threat-to-privacy

[10] Biometric Information Privacy Act (740 ILCS 14/7) Sec. 1 Short Title. This Act may be cited as the Biometric Information Act. (740 ILCS 14/10) Section 10. Definitions.

[11] Id.

[12] Section 312.2 Definitions.

[13] *See* 16 C.F.R. § 312.5(c).

[14] In a recent decision by the Illinois Supreme Court, Rosenbach v. Six Flags Entertainment Corp., the Court affirmed the right of private individuals to sue if a company collected his/her biometric data without his/her written consent, even if there was no "harm" to the individual. In this case, the mother of a 14-year-old minor sued the Six Flags theme park for collecting the fingerprints of her son in order to issue a season pass for the park without first obtaining written consent. While visitors to the park were told that they would need to provide fingerprints, and the context of the season pass program implied that consent would need to be given**, Six Flags did not explicitly receive written consent from the minor before issuing the season pass**. [Emphasis added]. In the lawsuit, Six Flags specifically acknowledged that no written consent was obtained – however, Six Flags also argued that the case did meet legal standards for demonstrating "harm." There was no data breach, there was no hack, and there was no physical or psychological harm that occurred to the boy as a result of giving the fingerprints. The Illinois Supreme Court filed a unanimous opinion that "harm to privacy" meets the legal definition required for "harm." Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186

CARU recommends that the Commission include biometrics in the definition of "personal information" and to apply COPPA protections because the full risks of collection and retention of children's biometric data could have dire ramifications in the event of a security breach or it could be used or sold for targeted, location-based advertising. A definition like the BIPA definition of biometric information could serve as a model to incorporate biometric information into COPPA's definition of personal information.

14. Should the definition of "Support for the internal operations of the website or online service" be modified?

Should additional activities be expressly permitted under the definition? For example, should the definition expressly include advertising attribution? Advertising attribution is the method used to determine whether an advertisement led the user to take a particular step, such as downloading an app.

During the last COPPA revision in 2013,[15] the Commission declined to add a list of proposed uses to the definition of support for internal operations because it believed that those functions were sufficiently covered by the revised definitional language.[16]

The Commission stated that it provided for future technical innovation by implementing the Voluntary Commission Approval Process in Section 312.12(b) of the COPPA Rule, which allows interested parties to file a request with the Commission for approval of additional activities to include within the definition of support for internal operations.[17]

CARU agrees with the Commission's position that the updated provisions adequately cover activities required to permit the smooth and optimal operation of websites and online services. CARU considers advertising attribution an activity that falls within the current definition as long as personal information is only collected and used for that specific purpose. Operators, like any other business, who advertise their product need to use advertising attribution.

While CARU regards the current definition as encompassing this activity, it would not oppose the addition of "advertising attribution" to the definitional language of "support for the internal operations of a website or online service."

15. Does § 312.2 correctly articulate the factors to consider in determining whether a website or online service is directed to children?

Do any of the current factors need to be clarified? Are there additional factors that should be considered? For example, should the definition be amended, consistent with the statute, to better address websites and online services that do not include traditionally child-oriented activities, but that have large numbers of child users? If so, what types of changes to the definition should be

[15]Federal Register Volume 78, Number 12 (Thursday, January 17, 2013) pp. 3979-3981.
[16] Ibid, pp. 3979-3981.
[17] Ibid, pp. 3979-3981.

considered? Are there other proposed amendments, consistent with the statute, for the Commission to consider to ensure children using these types of websites and online services receive COPPA protections?

The Commission should clarify the factors for determining whether a website or online service is directed to kids to better address websites and online services that do not include traditionally child-oriented activities but that have large numbers of child users.

The Internet has evolved in such a way that kids are everywhere, including – and importantly - places where we may not have expected or wanted them to go. Gone are the days of easily identifiable havens for children with animated characters, lullabies and simple games. Instead, children have infiltrated every corner of the Internet, including online services not meant for them. As a result, we have seen companies turn a blind eye to young audiences they never intended to have. In its capacity as a self-regulator, CARU has observed that it is the online services with the most pressing privacy issues that are often the most difficult to determine whether COPPA should apply.

For COPPA to remain effective in the future, we need to ensure that the factors that define what is "directed to kids" are updated to also cover online services that do not contain traditionally child-oriented activities such as social media or other platforms with user-generated content.

For instance, Google, LLC's (Google) YouTube website and app has been widely accepted publicly to be the top online destination for kids' video content (and was marketed as such by Google as documented in the FTC's recent investigation).[18] However, because YouTube did not technically fall within the current definition of a site or service "directed to kids" under the Rule, Google was able to avoid scrutiny until formal complaints were filed and, through its investigation, the FTC was able to prove actual knowledge.

Similarly, in the FTC's second largest COPPA settlement regarding the social media app TikTok f/k/a Musical.ly (referred to the FTC by CARU after its own investigation[19]), it was not easy to prove that COPPA should apply. In that case, TikTok collected and allowed children to share personal information without obtaining parental consent. To parents and the general public, it was easy to see children were present on the app in large numbers. In its own investigation, CARU observed a significant amount of public profiles of users who identified themselves as under 13 or who, by their photos, could be identified as younger than 13. Additionally, in statements to the press, the app's former-CEO admitted that he knew there were children using the app. However, even with these obvious factors, it was difficult to prove that the app was "directed to children" under the current Rule without additional evidence proving the operator had actual knowledge.

[18] FTC and the people of the state of New York by Letitia James, Attorney General of the state of New York vs. Google LLC and YouTube LLC, FTC File No. 1:19-cv-02642 (2019).
[19] Musical.ly Inc. (Musical.ly App), Case #6171, NAD/CARU Case Reports (April 2018).

CARU is mindful that the distinction is not always straightforward. There are thousands of apps in the app store[20] that include animated characters, bright colors and simple games, which happen to also appeal to a large number of adults. For example, the mobile app, Candy Crush, is a brightly colored, easy to play, animated puzzle game that is mainly played by adults whereas others, like the TikTok app, that feature user-generated videos, may not have been intended to be directed to kids but become a popular destination for under 13s. Similarly, in its case regarding the app Angry Birds, CARU determined that the app, which initially was not intended to be directed to kids, became directed to children when the app's creators began marketing toys and animated movies featuring the characters in the game.

For these reasons, CARU believes that the Commission needs to provide additional clarification when an online service that is not originally directed to children reaches a threshold that should no longer be overlooked and requires the protections of COPPA to apply. Simply put, the eight (8) factors currently used to determine whether an online service is directed to children must be updated to include additional considerations that were not contemplated (or even in use) 20 years ago. CARU recommends that additional factors should be considered such as requiring operators to periodically analyze and gather demographics on the actual audience of their online services.[21] This analysis may also include a closer review of consumer inquiries and complaints. An example of this data was relied upon by the FTC in their case against TikTok, finding that an abundance of complaints from parents about their under 13 children's use of the app was an indication that the app was directed to children.

Indeed, CARU believes that it is worth noting the importance of these factors and that they should be memorialized in the Rule itself rather than in the FTC's Business and Parents and Small Entity Compliance Guide (FAQs)[22], which although is a very helpful document when interpreting the law, does not provide an enforceable standard that can be relied upon in a case. CARU believes that by adding these steps, companies will be able to better prepare themselves. Additionally, doing so would also provide the FTC and CARU the backup they need to hold operators accountable for their COPPA compliance.

16. Has the 2013 addition, found in part (3) of the definition of "website or online service directed to children," which permits those sites that do not target children as their primary audience to age screen users, resulted in stronger protections for children's privacy? Should the Rule be more specific about the appropriate methods for determining the age of users?

CARU believes that the option to age-screen users and allow for an online service to simultaneously have under and over 13 users has not resulted in stronger protections for children while allowing them greater

[20] In addition to websites and YouTube videos.
[21] *See* COPPA FAQs (D.3.).
[22] See https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

options to participate in online culture. Allowing a mixed audience online service to direct child users to COPPA-compliant (and age-appropriate) sections of their services has proven to be a useful option, however implementation challenges, including increased costs, has limited its use in the marketplace. Ultimately, mere age-gating is not consistently effective, and a mixed-audience model is neither widely understood nor utilized.

The internet is constantly evolving and CARU wants to ensure that COPPA continues to apply in a way that makes sense. We are entering a new era and the industry needs to evolve with the realities with which we are faced. CARU uses its own voluntary self-regulatory investigations with companies to continue to move the conversation forward, which means adapting certain principles as technology evolves. For instance, in its case with Facebook, Inc., CARU held, based on its Guidelines, that a mechanism should be used to prevent kids from circumventing the age-screening process.[23]

CARU Guidelines also mandate that age should be asked in a neutral manner. Although the FTC has provided some guidance in its FAQs, there remains confusion in the industry as to what is considered a neutral method to ascertain age, especially since the trend in the international privacy community is that the least amount of information necessary to carry out the intended purpose should be collected. This has led CARU to re-consider its own recommendations that proscribe that age should be determined by collecting a full date of birth. For these reasons, CARU recommends that the Commission consider adding more specificity in the Rule regarding how age should be determined.

Today's children are tech savvy and sophisticated. It is literally "child's play" to breach an age gate for many children, especially "tweens." Accordingly, CARU believes that the FTC should encourage that the mixed audience model be used more often. Rather than simply age-screening kids where we know older kids will get through, companies should instead accept the reality and offer them an age-appropriate experience. The industry will be in a much better place if companies can no longer willfully disregard underage users.

Even when a site or service is not considered primarily directed to kids, CARU believes that the reality is that there are some (often many) children that attempt to access services that are accessed by older kids. It is for this reason that CARU believes that companies should have strong protections in place to anticipate access by children 13 and under. Companies, therefore, must focus on implementing procedures to ensure privacy-by-design from the start.

CARU believes that having an age gate should be the lowest bar for compliance with the law. While it may have been the gold standard for compliance in years past, today it should be the minimum that companies are required to do. Techniques that effectively restricted access and prevented children from

[23] . Facebook, Inc. (Facebook Mobile Application), Case #6274, NAD/CARU Case Reports (April 2019).

breaching protections are quickly becoming obsolete. For instance, CARU's Guidelines require age screens to implement a tracking mechanism to prevent kids from circumventing such precautions and simply back-buttoning and changing their age. While it is unclear how effective such a mechanism continues to be as children have become more sophisticated, CARU recommends that the current Rule be updated to include this requirement. Although it is listed as a best practice in the COPPA FAQ's, the FTC may not rely upon this document when building a case as it is not part of the actual regulation.

CARU believes that age gates should be part of a larger system to keep children safe on the internet because it is not a question of if kids will breach an age gate, it's a question of when. Companies should therefore incorporate privacy-by-design and systematic procedures of trust and safety from the ground up.

In CARU's Snapchat inquiry[24], it determined that when an online service makes additional efforts that ensure children's information is not collected, a company should be given due consideration regarding their efforts toward COPPA compliance.

In its case with Snapchat, CARU gave credence to the tight systems Snap implemented, that included an easy, in-app reporting tool permitting users to flag accounts that are believed to be underage as well as a robust trust and safety team that investigates all such reports. Behind the scenes, the company ensured that its legal and trust and safety departments worked closely with its product development teams to intentionally target the app to an older audience.

CARU recommends that all companies should endeavor to create a comprehensive culture of privacy.

H. Confidentiality, Security, and Integrity of Personal Information

28. Section 312.8 of the Rule requires operators to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from a child, and to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of the personal information, and who provide assurances that they will do so.

a. Have operators implemented sufficient safeguards to protect the confidentiality, security, and integrity of personal information collected from a child?

b. Is § 312.8 of the Rule clear and adequate? If not, how could it be improved, consistent with the Act's requirements? Should the Rule include more specific information security requirements, for example to require encryption of certain personal information?

[24] Snap Inc. (Snapchat App), Report #6297, *NAD/CARU Case Reports* (July 2019).

In its capacity as a Safe Harbor provider and self-regulator, CARU has found that companies participating in its safe harbor make a good faith effort to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children, However, more detailed guidance would be useful to determine what minimum standards are required to meet the standard of "reasonable" in this provision.

While Section 312.8 of the Rule does not define "reasonable procedures," recent actions including VTech Electronics Limited[25] and ClixSense.com,[26]among others, the FTC has provided more insight into what constitutes reasonable safeguards. These include:

- Avoiding misrepresentations about security;
- Implementing comprehensive data security and assessment programs verified by a competent third party;
- Designating an employee or team of employees to be responsible for data security,
- Training all employees on data security;
- Imposing appropriate security requirements on third party partners by contract;
- Regular assessments, testing, and monitoring to ensure that security checks are functioning effectively.

These cases provide a good general overview to industry of what procedures and policies operators should have in place. However, given the complexities of securing online data, CARU believes that additional guidance from the Commission, including specific security specifications such as encryption of certain personal information, would be of value to the business community as well as to the Safe Harbor programs tasked with ensuring companies are compliant with this provision.

I. Safe Harbors

29. Section 312.11(g) of the Rule provides that an operator will be deemed in compliance with the Rule's requirements if the operator complies with Commission-approved self-regulatory guidelines (the "safe harbor" process).

a. Has the safe harbor process been effective in enhancing compliance with the Rule?

b. Should the criteria for Commission approval of a safe harbor program currently enumerated in § 312.11(b) be modified in any way? To what extent should the Commission consider the financial structure and incentives of organizations operating safe harbors? Is there any evidence that the

[25] United States of America, Plaintiff vs. VTECH Electronics LTD, a corporation, and VTECH Electronics North America, LLC, a limited liability co., Case No: 1:18-cv-114.
[26] United States of America Before the FTC, Docket No. C-, In the Matter of James V. Grago Jr. individually and d/b/a/ ClixSens.com.

corporate structure of a safe harbor program impacts its effectiveness? Should the Commission consider applying any restrictions on the types of organizations that may operate safe harbors?

d. Should any other changes be made to the criteria for approval of self-regulatory guidelines, consistent with the Act's requirements?

e. Should the Commission consider any changes to the safe harbor monitoring process, including any changes to promote greater transparency?

f. Should the Rule include factors for the Commission to consider in revoking approval for a safe harbor program?

As the first FTC-approved COPPA Safe Harbor, over the years CARU has witnessed the positive effect Safe Harbors have in enhancing compliance with the Rule. Companies whose online services are directed to children or may attract a large audience of children join safe harbor programs because they understand the complexity of compliance and the need for assistance. However, the effectiveness is limited only to companies that are utilizing safe harbors which we estimate is less than 10 percent (10%) of all online service operators to whom COPPA would apply. The effectiveness could be broader if more operators were aware of COPPA and safe harbors. When the market is proliferated with non-compliant online services, it is challenging to explain to companies participating in safe harbors why they must make efforts to comply with COPPA. Shy of the FTC mandating that companies with online services directed to children join a safe harbor program, CARU asks that the FTC create a campaign to inform operators, third-party vendors and other companies in the ecosystem of child-directed online services about safe harbors. We believe that the more companies utilizing safe harbors, the more compliant the ecosystem will be. If the FTC implemented such an educational effort, CARU will fully participate and suggest that other safe harbors do the same.

CARU believes that the current criteria for approval of safe harbors is satisfactory, however more oversight should be considered. If the financial status of a safe harbor changes post FTC approval, the Commission should review what impact that financial status may have on the company's operation of their safe harbor. Although each FTC-approved safe harbor must submit essentially the same documents in their application to become a safe harbor, only the FTC truly knows the differences that exist on the operational side of each safe harbor. CARU suggests that the FTC consider enumerated criteria regarding minimum operating standards which may include how safe harbors are assessing compliance, how often they are monitoring and how they are communicating with their clients/members.

In furtherance of creating greater transparency, CARU will begin providing at least one annual report to the public detailing the types of compliance issues observed along with recommended solutions to achieve compliance. These reports will **not** specify company names, websites or apps or any other identifiable information. The purpose of these reports is to assist the FTC and the ecosystem in understanding the challenges companies are having in their compliance efforts. CARU suggests that the FTC require similar transparency by all safe harbors.

Revoking approval of an existing safe harbor is not something to be taken lightly. The impact of revocation ranges from the impact it has on the clients utilizing that safe harbor to the possible loss of income and jobs of the safe harbor operator. Nevertheless, the obligation of operating a safe harbor is of

great import and value, therefore the FTC should not shy away from exercising its power to revoke. It is appropriate for the FTC to set a high bar on the determining factors as all safe harbors should be aiming for such a bar. COPPA and the online children's environment can only benefit from additional oversight and high standards.

In closing, the one underlying factor in all of CARU's comments, as well as all the questions the FTC detailed in the Rule review, that we want to emphasize is the high cost of compliance: the cost for operators, vendors, platforms and safe harbors. CARU urges the FTC to keep the ongoing cost of compliance top of mind while considering any and all changes to the Rule. The smallest of operators in the children's space have great compliance challenges including the inability to afford the cost of joining a safe harbor. Therefore, the more information the FTC and safe harbors can provide to industry, the more likely we are to achieve a compliant ecosystem.

CARU appreciates the opportunity to submit this comment and welcomes any further discourse, including answering any additional questions from the FTC.

Yours truly,

Dona J. Fraser
Vice President, CARU
BBB National Programs, Inc.