COUNCIL OF BETTER BUSINESS BUREAUS, INC.
4200 Wilson Boulevard Arlington, VA 22203
845 Third Avenue New York, NY 10022
www.bbb.org www.caru.org www.bbbonline.org

June 11, 1999

Secretary
Federal Trade Commission
Room H-159
600 Pennsylvania Ave., NW
Washington, D.C. 20580

Re: Children's Online Privacy Protection Rule—Comment, P994504

Dear Mr. Secretary:

Enclosed is this original and five copies of the Council of Better Business Bureaus' comments on the Commission's proposed rules implementing the Children's Online Privacy Protection Act. Also enclosed is a 3 1/2-inch disk containing the comment in Word 97, Windows 98 format.

Introduction

The Council of Better Business Bureaus (CBBB) submits this comment on the Commission's proposed rules implementing the Children's Online Privacy Protection Act (COPPA). CBBB administers two of the most prominent programs in the nation that use self-regulation as a means for protection of the privacy of children who are asked to provide personal information online.

CBBB's Children's Advertising Review Unit (CARU), as part of a strategic alliance with the major advertising trade associations through the National Advertising Review Council (comprised of AAAA, AAF, ANA and CBBB), is the children's advertising arm of the advertising industry's advertising self-regulation program. CARU's 1997 Children's Advertising Guidelines for Interactive Electronic Media, **http://www.bbb.org/advertising/caruguid.html#media**, include the voluntary guidelines

for the online collection and use of personal information from children under 13 that were later borrowed in large part by Congress for COPPA, including the important requirements for parental consent. CARU's self-regulatory program was cited by the Commission as an example of successful industry self-regulation in its June 1998 report on the Commission's 1998 "sweep" of web sites directed to children. CARU monitors web sites directed to children, works with web operators to achieve compliance, publishes reports of its compliance reviews, and refers cases of non-compliance and refusals to cooperate to the Commission.

CBBB's online subsidiary, BBB*OnLine*, administers a program under which companies meeting BBB*OnLine* online privacy protection criteria may display a "seal" on their web sites to communicate their fair information practices to the public. Sites directed to children under 13 or which collect personal information from children known to be under 13 may display a special BBB*OnLine* Kid's Seal if the sites meet the additional qualifications regarding protection of children's privacy. BBB*OnLine* eligibility criteria, **http://www.bbbonline.org/businesses/privacy/eligibility.html**, insofar as they are applicable to children, are derived from CARU's leadership guidelines, additional requirements of COPPA, guidelines recommended by the Online Privacy Alliance, and from criteria generally applicable in the BBB*OnLine* privacy seal program.

Our comments on the proposed Rule are divided in two sections. The first responds to questions posed by the Commission regarding §§312.1-312.9. The second responds to questions concerning the safe harbor and related requirements at §312.10.

A. Sections 312.1-312.9

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

As a starting point, we are pleased that Commission's proposed rules under the COPPA so closely mirror CARU's Guidelines for Interactive Electronic. Since the adoption of our Interactive Guidelines in 1996, CARU has worked with more than 150 sites to bring them into compliance and we continue to monitor them as they create new content and features to ensure their continued commitment to our self-regulatory principles. CARU has also continued its routine patrolling of other child-directed Web sites to bring them into compliance as well. When CARU identifies sites whose privacy practices are inconsistent with our Guidelines, we begin an inquiry process to attempt to bring the site into accordance voluntarily. Overall, we have been successful in achieving voluntary compliance and in helping sites create interactive features that do not require children to provide identifying information. But where an operator refuses to implement necessary changes, CARU reports such findings publicly and refers the operator to the appropriate regulatory body, such as the Federal Trade Commission.[1]

Since its opening in March 1999, the BBB*OnLine* privacy seal program has already received over 340 applications, nearly 12% of which contain children's areas. In the short time since it's opening, BBB*OnLine* has granted Kid's Seals to companies such as The New York Times on the Web and Nickelodeon's Nick.com. BBB*OnLine* employs an extensive assessment and compliance review process prior to the grant of a Kid's Seal, and like CARU, has found success in obtaining voluntary compliance with its seal participants with all of the BBB*OnLine* Privacy Program standards. BBB*OnLine* also offers an alternative dispute resolution process, ongoing review, and substantial consequences in the instance of noncompliance including public revocation of a seal and referral to appropriate governmental agencies.

Through the efforts of CARU and the BBB*OnLine* Privacy Seal Program, we have found that many site operators are both willing and able to comply with our Guidelines and

[1] For a detailed description of the procedures used when CARU has initiated an inquiry into a site operator's information practices, see The National Advertising Division, Children's Advertising Review Unit & National Advertising Review Board Procedures for Voluntary Self-Regulation of National Advertising. They are available online at: **http://www.caru.org/nadproc.html**.

that there has been a growing recognition of the importance of establishing privacy protection programs in the last year. The success of industry-led privacy initiatives has been underscored by the recent release of the Georgetown University Internet Privacy Policy Survey, which found that 65.7 percent of web sites constituting 98.8 percent of consumer web traffic posted information practice statements.[2] Thus, given the significant improvements in establishing fair information practices by many members of the online world, coupled with the overall similarity between CARU's landmark Guidelines on Interactive Media (and therefore BBB*OnLine*'s requirements) and the Commission's proposed rules under COPPA, we are confident that the proposed rules will be successful in bettering children's privacy in the online world.

We have addressed the bulk of our comments on the proposed rules as answers to questions posed by the Commission. While we are in general agreement with the proposed rules, there are a few issues raised in the rulemaking that we believe may need further clarification or consideration by the Commission. We have addressed these issues below and in response to specific questions.

Section 312.2 Definition of Collection:

While we are in general agreement with the proposed definition of "collection," to include the direct or passive gathering of any personally identifiable information from a child, we are concerned by the potential scope as explained in the Commission's accompanying commentary. The Commission states that the term includes "all online requests for personal information regardless of whether the personal information is ultimately transmitted online or offline. Thus, it would include a situation where the web site or online service directs the child to print out a form, respond in writing to the questions, and mail the form back to the web site or online service."

Our programs support a reading of the statute that requires operators to obtain parental consent where offline collection of information will be used for site registration for

[2] The survey, released in May 1999 is online: **http://www.msb.edu/faculty/culnanm/gippshome.html**.

the purposes of allowing a child to engage in an online activity where personally identifiable information may be disclosed. Thus, where an operator provides a downloadable form or survey, to be returned via mail, and that is used to permit a child to gain access to a site to participate in an activity such as chat or a bulletin board, we strongly agree that such a registration must conform with the parental notice and consent rules. However, where a form or user submission does not pertain to an online activity, we are not convinced that application of the rules is advisable. For example, where users are provided with downloadable forms on Web sites for offline activities, such as essay writing or a color-in the images contest, it is unclear that the submission should trigger the COPPA rules. Similarly, where a form may be downloaded and the information is not collected online but is merely an advertisement for a contest that is also promoted in other media, such as television and magazines, a requirement that the downloaded version meet the COPPA rules – while other versions not – may create confusion amongst operators since COPPA pertains only to Internet based activities.

Moreover, a requirement that offline entries include parental consent where such submissions do not pertain to online information collection for the purposes of registration or participation in an online activity appears to be beyond the statutory scope of COPPA. Personal Information, as defined in the statute, pertains to "individually identifiable information about an individual collected online…" Moreover, the statutory definition of Disclosure pertains to information that may be revealed or disseminated "by any means by a public posting, through the Internet…"

Our conclusion that contests or forms that are merely advertised online (as well as other media), and that do not pertain to online activities or the potential posting of information, should not fall within the Commission's purview is also bolstered by the legislative history of the statute. The legislative history, as evidenced by Federal Trade Commission Chairman Robert Pitofsky's testimony before the Senate prior to COPPA's adoption, indicate that the statute was intended to apply to online collection of information because of the ease with which personally identifiable information may be collected and disseminated in the online world. Unlike online collections, CARU has avoided regulating

information collection for contests or other offline activities that require children to mail-in submissions from other traditional media. We believe that with regard to children's magazines submissions or cereal box top offers -- there is greater opportunity for parental mediation and less likelihood that children will divulge information without any parental knowledge of their activities. Additionally, there is less likelihood that such information will be publicly posted to third parties as is possible on the World Wide Web without parental knowledge. Thus, we conclude that the Commission should not apply the definition of "collection of information" to any activities not relating directly either to online registration or an online activity.

3. Section 312.2 defines "operator." (a) Is the definition sufficiently clear to provide notice as to who is covered by the Rule? (b) What is the impact of defining the term in this way?

We are in general agreement with the definition of "operator" and that an operator must disclose whether it shares, rents or sells information to "third parties." However, in determining whether an entity is an "operator" or "third party," we believe that the entity's corporate relationship to another operator, such as whether it is an affiliate, is a relevant factor for consideration by the Commission. The traditional legal definition of an affiliate is "with respect to any person, an entity that controls, is controlled by, or is under common control with such person." In contrast, a third party would be an entity that is not an affiliate and is related merely through privity of contract to the operator. Hence, the sharing of information by an operator with an affiliate that is under common control by a parent company, and that shares the same information collection and use policies should not be deemed third party use. A Commission determination that affiliates and other related corporate entities are third parties may generate confusion amongst operators and therefore lead to inconsistent treatment in privacy policies.

Under CARU's Guidelines, where the privacy practices differ among corporate relations or affiliates, the operator must disclose whether information will be shared and, if so, what the affiliate's policy is. The Guidelines state that "[w]hen personally identifiable information will be shared or distributed to third parties, except for parties that are agents or affiliates of the company or provide support for the internal operation of the Website and that

agree not to disclose or use the information for any other purpose, the company must obtain prior verifiable parental consent." Similarly, BBB*OnLine*'s requirements provide that "[s]eal participants must have a process in place to make unaffiliated third parties or corporate affiliates not covered by a common policy practice aware of the site's privacy policies when transferring individually identifiable information to such parties, and must describe that process in their Compliance Assessment."

Thus, the Commission should not treat affiliated corporate entities as third parties for the purposes of defining an operator. To avoid confusion, the Commission should instead require operators to disclose whether they share information with any parent company or affiliate (as well as a third party) that does not adhere to its stated information integrity and confidentiality practices.

4. Section 312.2 defines "personal information," in part, to include a persistent identifier, such as a customer number held in a cookie, or a processor serial number, where such identifier is associated with personal identifying information; an instant messenger user identifier; a screen name that reveals the individual's e-mail address; or a combination of a last name with other information such that the combination permits physical or online contacting. Are there additional identifiers that the Commission should add to the list?

Under our guidelines, the practice of collecting information from children through passive means (e.g. navigational tracking tools, browser files, etc.) must be disclosed to children and their parents along with an explanation of what information is collected directly by the site operator. We have required that CARU-compliant sites provide such notice both on their web sites and in any direct communications with parents to fulfill notice and consent requirements if there is a registration process for children. Similarly, such notice is a requirement of BBB*OnLine* seal program participants. We therefore concur with the Commission's definition of personally identifiable information as including "passive gathering tools," such as cookies, where they are used in conjunction with individually identifiable information to create a personal profile.

We are currently unaware of any additional "passive" identifiers that should be considered at this time.

Notice

5. Section 312.4(b) lists an operator's obligations with respect to the online placement of the notice of its information practices. (a) Are there other effective ways of placing notices that should be included in the proposed rule?

Under CARU's Guidelines and BBB*OnLine*'s program requirements, information collection and use practices must be clearly disclosed, along with the means of correcting or removing the information. The disclosure notice must be prominent and readily accessible from the home page and from any page where information is collected. Beyond these requirements about placement of privacy policies we do not restrict where the notice must be placed on a Web page and instead require that the hyperlink to the policy use a prominent heading, such as, "Privacy," or "Our Privacy Policy," "Note to Parents" or a similar designation.

Thus, while we are in agreement with the proposed requirements that privacy policies must be clearly labeled and placed in a prominent location on the site's home page and where ever information is collected, we do not believe that it is necessary to prevent a site owner from placing the link on a portion of the home page that requires scrolling to reach. Such a restriction is contrary to developing industry privacy practices since many sites that feature privacy polices provide links to such policies at the bottom of their home page, where they also provide copyright or other legal notices. We have provided a few examples of such CARU-compliant sites that provide privacy links at the bottom of their home pages:

Scholastic, Inc.'s site at http://www.scholastic.com

Mattel, Inc.'s site at http://www.mattel.com/.

Sports Illustrated for Kids at http://www.siforkids.com/.

MARS, Inc.'s M&M's site at http://www.m-ms.com/.

Able Minds, Inc. site "CyberKids" at http://www.cyberkids.com.

Random House, Inc.'s "Kids@Random" at http://www.randomhouse.com/kids/.

Nabisco's site, "Nabisco for kids" at http://www.nabiscokids.com.

General Mill's children's site at http://www.YouRuleSchool.com/.

Ohio Art, Inc.'s site "World of Toys" http://www.world-of-toys.com.

Nestle, Inc.'s "Butterfinger" site at http://www.butterfinger.com.

Media Bridge Gamekids site at http://www.gamekids.com.

Similarly, the online site for **Nickelodeon, at http://www.nick.com**, which is the first recipient of the BBB*OnLine* Kid's online privacy seal, contains a link to its privacy policy at the bottom of its home page, above the privacy seal.

Since each of these sites provide clear and conspicuous notice, further restrictions on where notices must be physically placed are unnecessary at this time given the commitment to strong information privacy practices by these and other compliant site operators. Similarly, it is unclear that the Commission should propose other required methods of placing privacy notices at this time. Where an operator has complied with the substantive requirements, and the notice is clear and conspicuous, further non-substantive requirements at this time may fail to take into account emerging methods of providing notices that may enhance user access to such policies and may thwart development of better mechanisms.

(b) How can operators make their links to privacy policies informative for parents and children?

CARU's Guidelines emphasize that advertisers/operators that create child-directed material in any media "should always take into account the level of knowledge, sophistication and maturity of the audience to which their message is primarily directed. Younger children may have a limited capacity for evaluating the credibility of information they receive. They also may lack the ability to understand the nature of the information they provide." The BBB*OnLine* requirements are that all notices directed to children must be in "language easily understood by a child." Operators may make their privacy policies more informative for all users by meeting the CARU and BBB*OnLine* requirements that sites create notices that are "clearly worded, legible and prominent" and should avoid the use of sophisticated terms that may not be comprehended by a child audience. Where technology permits, we also

encourage site operators to use audio and visual tools as well as demonstrative disclosures to help children better understand their messages.

One method that some CARU-compliant sites have used to make their links to policies more informative is through the use of graphic illustrations that teach children the importance of keeping personally identifiable information private. For example, CARU recently worked with Chevron, Inc. when it sought to create a children's animated site about cars and trucks at **http://www.chevroncars.com/.** In creating its privacy policy, Chevron created an animated feature and character "Wally the Warning Squirrel" that appears throughout the site to remind children about privacy issues and informs them if they are being asked to provide personally identifiable information. Wally the Warning Squirrel also reminds children that they should ask a parent for permission before giving out information anywhere online and that they are not required to provide information to participate in activities on the Chevron Cars site. The animated reminders are also accompanied by a registration process that requires parental consent for the collection and use of the child's information.

To ensure that a site's good privacy practices are not compromised through linking to others, CARU discourages compliant sites from hyper-linking to sites that may collect personal information without satisfying disclosure and consent requirements. But even where sites link to compliant sites, there may be no way to predict where the use of successive links on successive pages will lead. Thus, CARU encourages sites to feature "splash screens" or "bumper screens" before connecting to hyper-linked providing prominent warnings to children that they should never give out personally identifiable information without parental permission. BBB*OnLine* similarly addresses hyper-linking by requiring seal participants to either avoid linking to the pages of other websites that do not meet certain core privacy requirements, or alternately providing a bumper screen on all links leading from a designated children's area. At the Nickelodeon site, for example, bumper screens are used to warn children that they have chosen a hyperlink to an advertisement. Additionally, bumper screens appear before a user may follow an offsite hyperlink. The bumper screen states:

You're leaving nick.com to go to

another Nickelodeon web site that
may have stuff for grownups as well
as kids.

Click "GO"

Remember: Always check with your parents before you give information online and never give out your full-name, phone number, or address on the Internet because that stuff is yours and it's private!!!

While the Commission should not mandate the use of features such as bumper screens or other demonstrative techniques, our experience in working with our supporters and other sites is that many sites committed to promoting safe and rewarding use of the World Wide Web by children may voluntarily choose to create such features.

7. Section 312.4(b)(2)(iv) requires an operator to state whether third parties to whom it discloses personal information have agreed to maintain the confidentiality, security, and integrity of that information. How much detail should an operator be required to disclose about third parties' information practices?

We generally agree that parents must be provided sufficient information to provide informed consent about whether to permit their child to register at a particular site. In some cases, however, a notice or warning to review third parties' privacy policies may be a sufficient means for alerting the parent and child of the need to determine the third parties' practices.

8. Section 312.4(b)(2)(vi) requires an operator's notice to state that the parent has the right to review personal information provided by his or her child and to make changes to and/or have that information deleted, and to describe how the parent can do so. Is this information needed in the notice on the web site or online service, or should it be included only in the notice provided directly to the parent under section 312.4(c)?

Under our Guidelines, onsite notice about privacy practices, as well as direct parental notification, must inform the parent about their right to make changes to information collected about their child, along with instructions on how they may do so or how they may delete any data already collected. There are clear benefits to including such information in both the on-

site policy and in notices directed to parents to obtain consent for their child's registration. For parents who are able to spend time "surfing" the web with their children, notices placed directly on a site in the privacy policy may help them to evaluate, in advance, whether their children should register or frequent the site. But because many parents may not be "cyber-savvy" or may have children who access the World Wide Web from outside their homes, at school or the public library, including detailed information in parental notices is also extremely important.

9. Section 312.4(c) lists several methods an operator may employ to provide direct notice to a parent whose child wants to provide personal information or from whose child the operator wishes to collect personal information. Are there other, equally effective methods of providing notice to parents that the Commission should consider?

The "reasonable efforts" standard provided in section 312.4(c) is substantially similar to CARU's standard -- devised in 1997 -- after CARU began its efforts to promote industry self-regulation in the online environment. It has been CARU's experience, that where a parent does not have online access to e-mail, allowing children to download a consent form may provide sufficient methods of allowing that child to participate by giving the parent alternative methods to register the child offline (by mail, telephone or facsimile). CARU and BBB*OnLine* both agree that "reasonable efforts" to send parents notice under this section should include a downloadable form and an e-mail form. However, it is unclear that the Commission's suggestion about sending notices to a parent or guardian's home address is appropriate at this time. Sending notices via mail will require an operator to collect home address information from children seeking to register which would violate CARU's Guidelines' restriction against site operators from collecting offline contact information directly from children.

We will continue to monitor developing methods of sending notices, but are unaware of any other viable methods, that would not be overly invasive, at this time.

10. Section 312.4(c)(1) details the information that must be included in the notice to the parent. (a) What, if any, of this information is unnecessary?

We are in general agreement with the contents of the parental notice as proposed by the Commission.

(b) What, if any, other information should be included in the notice to the parent?

In addition to the parental notice requirements listed by the Commission, notices should also include warnings to parents that where a site operator does not disclose a child's personally identifiable information in interactive areas such as chat rooms or bulletin boards (or to other parties), children should be instructed not to post such information about themselves. Parents should be aware that even where interactive areas are "monitored," an operator cannot be liable for any personally identifiable information posted voluntarily by the child where such information is not requested by the operator and the operator has taken reasonable measures to safeguard the user's identifying information (e.g. by requiring users to use screen names without an e-mail address or last name associated with it when posting in chat areas).

Moreover, sites that provide interactive forums should inform parents whether user information will be disclosed or whether disciplinary action will be taken in the event that their child posts inappropriate information. Sites should also inform parents that information collected or posted by their child may be disclosed where required by law.

11. Section 312.5 requires the operator to send a new notice and request for consent to parents in certain circumstances. The proposal covers instances where the operator wishes to use the information in a manner that was not included in the original notice, such as disclosing it to parties not covered by the original consent, including parties created by a merger or other corporate combination involving existing operators or third parties. (a) Does this formulation sufficiently protect children's privacy given the high merger activity in this industry?

Where a merger may effect the uses or integrity of information collected because the parties have changed the policy as previously disclosed, parental notification may be necessary. Under both CARU's Guidelines and the BBB*OnLine* Program requirements, whenever a party changes its information practices or intends to use information in a manner inconsistent with an original notice, parental consent must be obtained. Absent a change in information practices, direct notice (e.g., via e-mail) of a merger may be unnecessary. Such

precautions should protect the integrity of collected information despite any corporate identity changes.

(b) Is this formulation more burdensome than necessary to protect those interests?

To the extent that a merger will not have a direct effect on the information practices, and information will not be sold or shared with additional parties, sending new notice to parents may be burdensome both for the operators and for parents that may not wish to receive messages where additional consent is unnecessary.

(c) Is there an alternative formulation that would sufficiently protect children's privacy without unnecessarily burdening operators?

Site operators should also post information about changes in management directly on their sites in their privacy policies. Until such a time when additional consent is necessary because information will be used in a new manner, children's privacy may be safeguarded without requiring additional information be sent to parents.

Parental Consent

12. Section 312.5(a)(2) requires operators to give the parent the opportunity to consent to the collection and use of the child's personal information without consenting to the disclosure of that information to third parties. Should the rule also require that the parent be given the option to refuse to consent to different internal uses of the child's personal information by the operator?

Parents should have the opportunity to request that all information about their children be removed whether the information will be shared with third parties or used only for internal purposes. It may be unnecessary for the Commission to require that operators provide parents the opportunity to refuse certain internal uses since parents may refuse to allow any internal uses altogether. Moreover, many sites currently permit registrants to opt-in for certain specific uses. For example, a user may provide information in a contest area and the operator may state that the information will only be used for the purpose of contacting a winner. Similarly, the user may provide e-mail information only to receive a newsletter and choose not to receive any product information.

Many sites that CARU has monitored as a result of our routine patrolling allow children to participate in site activities without registering any personally identifiable information or by permitting a child to participate using only a screen name (without requiring any personal information). Thus, where parents do not wish to allow any uses of their child's personally identifiable information online their children may still use online resources.

13. The commentary on Section 312.5(b) identifies a number of methods an operator might use to obtain verifiable parental consent. (a) Are the methods listed in the commentary easy to implement?

The methods for obtaining "verifiable parental consent" proposed by the Commission include: having a parent send a consent form via postal mail; facsimile; using a credit card in connection with a transaction; having a parent call a toll-free telephone number; or through an e-mail based mechanism using a digital signature.

Although there are CARU-compliant sites that have implemented each of these methods, it unclear whether these methods will be appropriate for all sites since the costs of implementing such mechanisms may be considerable, especially for smaller site operators. One of the incredible aspects of the World Wide Web is that it provides smaller sites an opportunity to provide rich content that may surpass the quality of traditional publishers or media providers. By requiring smaller operators to establish certain verification methods, it may become increasingly difficult for some operators to provide children with certain interactive features.

Thus, CBBB believes that there is a significant advantage in allowing a certain degree of flexibility in the type of methods used to obtain parental consent. Such flexibility should also permit sites that do not share, rent or sell information and do not provide any features that would permit third parties to directly contact children -- such as chat rooms -- to use an e-mail based mechanism for providing parental notice. However, we do not believe that allowing for parental consent via e-mail is adequate since it is not verifiable. Instead, the Commission should permit sites to use any combination of the methods suggested in order to obtain parental consent.

(b) What are the costs and benefits of using the methods listed?

The costs of obtaining consent via mail, facsimile or through a toll-free registration phone numbers include: added staff to input such information (since receiving consent online via e-mail may be automated); an added delay in time for registering a child; and difficulty in verifying the identity of the consent provider. Credit card verification methods may only be effective where there is a sale involved since credit card companies charge operators a fee for each transaction.

The benefits of using such methods to obtain consent are that they create an extra layer between the operator and a child and that there is less likelihood that a younger child will attempt to falsify consent.

(c) Are there studies or other sources of data showing the feasibility, costs, and/or benefits of the methods listed?

We have not conducted any such studies.

(d) Are there existing methods, or methods in development, to adequately verify consent using an e-mail based mechanism?

Please see our response to (f) below.

(e) What are the costs and benefits of obtaining consent using an e-mail-based mechanism?

Please see our response to Question 14.

(f) To what extent is digital signature technology in use now? Are there obstacles to the general commercial availability or use of digital signature technology?

Currently, it appears that the use of digital signature technology is still in limited use, mostly in business-to-business transactions. It is unclear that even larger children's sites are in a position to use such mechanisms, both because of the costs and because it may be premature to adopt any particular system at this time.

14. With respect to methods of obtaining verifiable parental consent, should the Commission allow greater flexibility in mechanisms used to obtain verifiable parental

consent in cases where the operator does not disclose children's personal information to third parties or enable a child to make such information publicly available through, for example, a chat room or bulletin board?

Protecting children from divulging personally identifiable information in the online environment has been one of our primary concerns in devising both CARU's Guidelines for Interactive Media and the BBB*OnLine* Kid's Seal. At the same time, we also recognize the importance of helping children develop skills and in learning in an increasingly interactive world. Thus, where a child registers with a site by creating a screen name and provides an e-mail address solely for the purpose of receiving an electronic newsletter, there is a benefit in reducing the difficulty for parents to respond immediately to a request for consent by a site operator by permitting e-mail notice.

We therefore believe that under limited circumstances, it may be appropriate for the Commission to allow greater flexibility in mechanisms used to obtain parental consent. For example, where information will not be disclosed to third parties and where information will not be posted online in any manner that would permit children to be directly contacted by or shared with third parties, CARU and the BBB*OnLine* Kid's Seal program permit sites to provide notice to parents via electronic mail.

Allowing a certain degree of flexibility also benefits smaller operators, with less elaborate sites that do not include bulletin boards or chat features. These sites may be less able to absorb the costs of setting up toll-free registration phone numbers or the costs of inputting offline parental consent obtained through the mail or by facsimile. The burden of obtaining hard-copy consent is considerable and may be overwhelming for small operators that do not market products on their sites and do not offer chat, bulletin board or other highly interactive features that could enable a child to communicate directly with others through the site. However, we do not believe that allowing for parental consent via e-mail should be the only method or the appropriate method in all circumstances. Our response to question 22 provides a discussion of some alternative methods of verifying parental consent offline where children are asked for other personally identifying information or are registering for the use of services that may permit third parties to contact them directly. These methods have been

implemented by some CARU-compliant sites already and may be necessary in certain circumstances.

15. Are there any studies or other sources of data regarding the ease or frequency with which children can fabricate parental consent using any of the methods discussed in the proposed rule?

We are not aware of any such studies. However, the use of offline parental consent mechanisms, where sensitive information may be collected by a child or where posting of a child's information would permit third parties to directly contact the child (e.g. bulletin boards or chat rooms that reveal e-mail addresses) could minimize any potential risk of fabricated consent. For example, where a site has implemented a toll-free, call-in registration system for parents, operators may be better able to identify child callers and instruct them to have a parent or guardian call instead. Ultimately, where sites take reasonable care in instituting children's privacy practices we urge the Commission to adopt the policy that site operators are not responsible for fraudulent information or acts committed by users.

16. Would additional research regarding children's behavior in the online environment be useful in assessing the appropriateness of various parental consent mechanisms?

Such research may be beneficial to gauge the success of emerging parental contact/ consent mechanisms as they develop and to measure the success of COPPA's implementation. Since CARU first adopted Guidelines for Interactive Media in 1997, we have required that "reasonable efforts" be made to provide notice and choice to parents when information is collected from children online. The "reasonable efforts" standard has been an evolving one and we continually consider changes in the media environment to determine whether the methods that we endorse are appropriate in light of any new technological developments.

17. Section 312.5(c)(1) allows an exception to prior parental consent where an operator collects the name or online contact information of a parent or child to be used for the sole purpose of obtaining parental consent or providing notice under this rule. Under this exception, if an operator has not obtained parental consent after a "reasonable time" from the date of the information collection, the operator must delete the information from its records. (a) What is a reasonable time for the purpose of this requirement? On what is the estimate of a "reasonable time" based?

Because the nature of activities for which consent may be obtained by a site varies depending on whether the activity is ongoing or short-term, we believe there should be flexibility in the amount of time that an operator retains parental consent contact information. For example, where a site collects parental contact information for the purpose of administrating a contest that is of a six month duration, a reasonable time to hold onto parental information would be until fulfillment of the contest is complete. However, where a site attempts to obtain parental consent for the purposes of an ongoing site activity, such as creating a chat room profile for a child, a reasonable time that the operator may hold onto such information should provide sufficient time for smaller operators that may not have sufficient staff to expunge lists on a weekly or monthly basis.

One question that we believe warrants further clarification by the Commission is how long site operators must retain parental consent. Thus, where a parent completes a registration for a child, will operators be required to hold onto the parental consent forms indefinitely? Is there a reasonable time after which operators may delete such information?

(b) Alternatively, should an operator be required to maintain a "do-not-contact" list so as to avoid sending multiple requests for consent to a parent who has previously refused to consent? What are the costs and benefits of such a do-not-contact list?

One of the remarkable aspects of the World Wide Web is the ease with which the content of sites may change. Sites that may feature less educational content or age appropriate content today may provide a wealth of information and resources for children weeks tomorrow. Thus, while a parent may discourage a child from registering or using a site now, they may later encourage the child to use the same site. Therefore, from a practical perspective, a do-not-contact list may not always be desirable at this time.

For small-site operators, maintaining such lists of "do-not-contact" individuals may be extremely burdensome to manage and costly. Moreover, many sites that are compliant with our guidelines immediately send a parent notification after a child has attempted to register with the site. If site managers were required to check whether the parent or guardian's name appears on a "do-not-call" list, the child's ability to register may be further

delayed. Additionally, maintaining a "do-not-contact" list may require operators to gather more profile information about parents than they currently need to in order to obtain parental consent (since an operator may only collect a the parent's e-mail address without their name or offline address to obtain consent). A "do-not-contact" list may require them to have the individual's name or offline contact information as well thereby increasing the amount of intrusiveness into parent's privacy as well.

Questions 18-21 (answered together)

18. *Section 1303(b)(2)(B) of the Children's Online Privacy Protection Act and Section 312.5(c)(1) of the proposed Rule allow an operator to collect the name or online contact information of a parent or child solely for the purpose of obtaining parental consent or providing notice. Are there circumstances that would necessitate collection of the child's online contact information rather than the parent's?*

19. Section 312.5(c)(4) allows an exception to prior parental consent where an operator collects information from a child in order to protect the safety of a child participant on its site. What specific circumstances should trigger this exception?

20. *Section 312.5(c)(5) allows an exception to prior parental consent where an operator collects information from a child for certain limited purposes. To what extent is a child's name or e-mail address necessary: (a) to protect the security of the website; (b) to aid in the judicial process; (c) to aid law enforcement?*

21. *Section 1303(b)(2)(c)(ii) of the Children's Online Privacy Protection Act authorizes the Commission to allow other exceptions to prior parental consent in this rule "in circumstances as the Commission may determine are appropriate, taking into account the benefits to the child of access to information and services, and risks to security and privacy of the child." What other circumstances might merit such an exception? What are the risks and benefits of creating such an exception?*

Where information will not be collected in a form that may be retrieved for various internal or third party uses, there may be a need for limited exceptions to the parental notice and consent rule to permit sites to collect or retain a child user's e-mail or other identifying information to shield itself from legal liability for the user's conduct or to comply with a valid judicial subpoena based on the user's conduct.

For example, many sites offer users the ability to send electronic postcards to others through their sites. With these features, users may send friends or family greetings for birthdays, mother's day or any other purpose. In order to permit child users to send cards

real-time (since parental consent verification may take a significant amount of time) some sites explicitly state that they do not retain the e-mail addresses of either the sender or the recipient thereby avoiding COPPA's requirements since there is no "collection of information." Other operators have expressed concern that by failing to require the sender's e-mail address, messages sent by a site user will appear to have been originated by the operator and neither the recipient nor the operator will be able to identify the sender in the event that the sender forwards a postcard containing an inappropriate or offensive message. Thus, to avoid liability or to allow recipients to identify who has sent them messages, operators may wish to retain the sender's e-mail address with an explicit statement that such information will not be used for any other purpose. Such retention should not require parental notice and consent where there is a promise that the information is retained only for security or legal purposes.

Thus, the Commission should consider creating limited exception for interactive features, where information is only retained to shield a site from user-created liability (e.g., posting inappropriate content on a bulletin board or in a children's chat area). The exception should be conditioned on the operator's commitment that the information collected under an exception will not be used for any other internal or third party use, will be maintained with adequate security and will only be used to protect the operator from legal liability or to comply with a judicial subpoena. Any exceptions must also remain narrow in scope so as to avoid the creation of too many exceptions which may confuse operators and parents.

22. *Section 312.6 gives a parent whose child has provided personal information to a web site the right, upon proper identification of that parent, to review the personal information provided by the child. The commentary on this section lists several methods an operator may employ to obtain proper identification of a parent. (a) Are there any other methods of identification that the Commission should consider?*

Where a parent has requested that an operator provide them with access to any information collected by the site about their child, the proposed rule states that operator must "ensure that the requester is a parent or that child, taking into account available technology." The Commission suggests that one method an operator could verify that an individual is the parent of a child is by providing the operator with a copy of the parent's driver's license,

showing that the parent and child live at the same address. It is unclear at this time whether such a system is practical or feasible since such method would require operators to verify identity based on mailed-in copies of identification, which would not only take a significant amount of time, but would also be of less help where a parent or guardian does not live with his/her child or has a different surname. Moreover, many operators do not collect children's offline addresses so there can be no comparison of a parent's address with a child's.

Similarly, at this time it is unclear that there are feasible or effective methods of doing online identity verification. While such methods are currently under development, mandating the use of certain methods, such as credit card verification, which may only be applicable where there is a commercial transaction involved in the registration process, may currently be too burdensome for small operators and may also thwart the development of alternative methods of verification. Rather than mandating the use of certain technologies, some CARU-compliant sites have found ways to facilitate parental access to their child's information without requiring online identification.

An alternative method to allow parental access to their child's profile without using an identity verification mechanism (such as appearing in person with valid photo identification) is to require the parent to create a password when registering their child that they would use to preview the child's personal profile. Thus, only the parent would have access to the information to modify or remove the child's information.

One example of a CARU-compliant site using such a mechanism is **Headbone Zone at http://www.headbone.com/.** For a child to use certain interactive features at Head Bone Zone such as the HBZ chat and the HBZ pager, a parent must complete an offline registration process by using a toll-free number or via facsimile. At the time of registration the parent creates the child's profile along with a password to be used for log-in and to make changes or delete the child's profile. The password is not disclosed by the operator to any other parties, thereby providing a parent with access to the child's account information at all times.

(b) In particular, are there other methods that could constitute proper identification in non-traditional family situations (e.g., where the child and parent do not live at the same address or where someone other than a parent is the legal guardian)?

Where a site establishes a pre-registration password system (described above), parents or guardians may be able to access a child's information without having to provide an offline identification. Similarly, we believe that other methods of verification or site registration will emerge that may provide for greater flexibility both for parents and operators.

(c) Are there any technological advances under development that may ease the process of obtaining proper identification of a parent?

Many e-commerce and privacy experts expect that the use of digital signatures or trusted third parties will help ease the current difficulties in verifying identification online. At this time, however, it appears that such technologies are in their infancy and that they are in limited use, mostly in business-to-business transactions. Other privacy enhancing technologies that are still under development include the World Wide Web Consortium (W3C)'s Platform for Privacy Preferences Project (P3P)[3]. P3P provides a framework for informed online exchanges, whereby a user exercises preferences over a Web sites' privacy practices and tailors the type of information that is released to the site. Thus, the user negotiates whether the site has met pre-established criteria on what information he or she is willing to exchange and under what circumstances.

We will continue to monitor such developments and encourage their use by operators as the technologies further mature and become feasible even for small sites. Until such a time, we believe it is premature for the Commission to mandate the use of such online verification mechanisms.

Prohibition against conditioning a child's participation on collection of personal information

[3] See W3C's "P3P in a Nutshell" online at: <http://www.w3.org/P3P/Overview.html> and Architecture is Policy Case Study: Cooperative development as a means for a standards-based Implementation for Privacy on the Internet by the Electronic Frontier Foundation, online at: **http://www.eff.org/privacypaper/.**

23. Section 312.7 prohibits operator from 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 to participate in such activity. What kinds of information do sites collect as a condition of allowing a child to participate in a game, contest, chat room, or other online activity?

As previously noted, since 1997, when CARU first instituted its Guidelines for Interactive Electronic Media, we have monitored and worked with more than 150 child-directed sites to secure compliance with our Guidelines. The CBBB is pleased with the progress that site operators have made in devising comprehensive privacy protections since the release of CARU's Guidelines and the launch of the BBB*OnLine* program this year. We will continue to encourage site operators to embrace our standards for privacy protection, through compliance with our guidelines, enrolling in the BBB*OnLine* Kids Privacy Seal Program and by continuing CARU's routine patrolling of children's sites.

In addition to posting privacy policies, through our efforts, many sites now collect no more information than necessary to permit children to participate in site activities and allow them to create screen names that allow them to post messages or play games online without revealing personally identifiable information. To underscore these achievements, we have listed a few CARU-compliant sites that allow children to participate in activities without registering and that provide COPPA compliant parental notice and consent where registration is required because of the nature of the activity. Many of these sites have been ranked among the top hundred children's sites.

Purple Moon Place at http://www.purple-moon.com/. Purple Moon is the only web site 100% dedicated to 8-to-12-year-old girls. Among this sites features are online games, e - postcards that may be shared with friends and bulletin boards (that require offline parental registration).

The Public Broadcasting Station's children's site at http://www.pbs.org/kids. This site features educational programming information, activities such as "Fun and Games," with a coloring section, a jokes section, a kareoke sing-a-long area; "Babble On," an interactive

writing section, and a pre-school activities section. The site also includes a section on technical literacy for children which teaches "Internet know-how."

Mattel's Hot Wheels Web site at http://www.hotwheels.com/. This site allows children to customize their own web page using only a screen name.

Sports Illustrated for Kids at http://www.siforkids.com/**.** This site is the online counterpart to the magazine directed at younger sports fans. SI for Kids offers numerous online sports games, articles, user writing submission features that children may use without any registration.

MARS, Inc.'s M&M's site http://www.m-ms.com/. Site features M & M's trivia, virtual factory tours explaining how the chocolates are made, recipes, the M & M's Motor Sports Channel, games, comics, a virtual art room that can be used without registration.

Crayola Crayon's web site at http://www.crayola.com**.** At this site, children may color pictures online and download pictures to color offline, find fun facts about crayons, stories, play games such as "Color Match'n Madness – all without providing personally identifiable information.

MamaMedia, Inc.'s site at: http://www.mamamedia.com**.** This site contains digital tools that let kids create their own stories and plays, artwork and characters. It contains many activities for very young Web users that do not require any information disclosure to participate.

While we are extremely encouraged by the efforts of these sites, at the same time, we acknowledge that some sites continue to engage in information collection practices that violate both COPPA and CARU Guidelines. Through our routine patrolling of online kids

sites, CARU has found that certain sites continue to collect information from children, such as e-mail addresses, offline addresses and phone numbers. Moreover, some sites that feature chat rooms, pen pal services or that allow users to create their own home pages often permit children to sign-up for services and post information online without satisfying the parental notice and consent requirements.

When CARU identifies such non-compliant sites, we begin our inquiry process to attempt to bring the site in compliance with our Guidelines voluntarily. Overall, we have been successful in achieving such voluntary compliance and in helping sites create interactive features without requiring children to provide identifying information or requiring that the sites obtain verifiable parental consent before allowing children to participate. But where an operator refuses to implement necessary changes, CARU reports such findings publicly and refers the operator to the appropriate regulatory body (in some cases, the Federal Trade Commission). BBB*OnLine* procedures also require referral of non-compliance to appropriate governmental agencies.

One example of a recent inquiry where CARU reported a site to the Federal Trade Commission because the operator failed to implement our Guidelines was with the site "Talk City," at **http://www.talkcity.com**.[4] The Talk City site came to our attention through routine patrolling of the Internet. CARU's review of the site found that it contained numerous areas where visitors can enter information about themselves, and communicate directly with each other, either in chat rooms (kids and adult directed), message boards (kid and adult directed) or their own home-pages administered by Talk City.

We have found similar problems on other sites as well and continue to reach out to operators to bring them into compliance. Our organization is committed to continuing the process of working with site operators to implement both our guidelines and to assist Website

[4] The full decision of the Children's Advertising Review Unit in this matter is published in the NAD Case Report, May 1999 (published by the National Advertising Division of the Council of Better Business Bureaus).

operators in complying with COPPA, and believe that we have substantially affected the number of sites that engage in unfair information collection practices from children.

B. Section 312.10—Safe Harbor Requirements

General Comments

CBBB enthusiastically supports the concept of the "safe harbor" as an effective tool to encourage and reward industry self-regulation. It is recognition by the Congress and the Commission that voluntary compliance has more staying power, more flexibility and best conserves limited government resources better devoted to significant law enforcement needs.

At the same time, if the standards for qualification as a safe harbor are not sufficiently rigorous, that might unintentionally result in a false sense of security by the public and create disincentives for participation in credible, thorough programs. CBBB's November 19, 1998 comments to the Department of Commerce (DOC) with respect to the DOC-European Union safe harbor negotiations sum up our views on the need for meaningful standards for self-regulation programs:

> "Our experience in operating a "seal" program online in connection with helping consumers find reliable companies, **http://www.bbbonline.org/businesses/reliability/index.html**, is that many new companies, inexperienced in the consumer protection field, have seen the Internet as an attractive entrepreneurial opportunity, but too many do not deliver or even attempt to deliver a high integrity service. There have even been occasional "seal givers" that appear to be "shills" for their participating companies. The result in these situations, of course, is improper and dangerous reliance on these "seals" by unwary consumers, and a risk of lessening respect for online consumer protection efforts in general. It can be expected that online privacy seal and other private sector enforcement efforts will encounter similar problems, and these may even be greater because of the likely widespread public education efforts underway or planned by the private sector and government aimed at recommending to consumers that they look for a "seal" or other indicator of an online privacy enforcement mechanism. Moreover, without rigorous and somewhat more detailed standards defining acceptable enforcement programs, a principle of "adverse selection" may drive businesses to the weakest or less demanding of the

programs, thereby depriving the public of needed minimum protections and risking the eventual collapse of the safe harbor concept."

With these considerations in mind, the CBBB commends the Commission for an excellent start in development of the safe harbor framework, and offers the following comments and suggestions for possible improvements:

§312.10(b)(1)

This section requires self-regulatory guidelines seeking safe harbor approval to require that "operators subject to the guidelines ('subject operators') implement the protections afforded children under this Rule." Some additional clarification would be helpful.

Is an operator "subject to" approved self-regulatory guidelines simply if the operator collects information from children, or must an operator and/or the self-regulatory program publicly declare the intent of the operator to be bound by the guidelines? We assume (and recommend) the latter. Unless a public declaration of some sort were required, the self-regulatory program would have no reliable vehicle for testing compliance or not, and the public would be unable to rely on the self-regulatory program as a basis for making a judgment to visit the web site or not. Of course, any declaration of an operator that it is subject to the guidelines (say, for example, by display of a seal or a membership insignia) would need to be consistent with the rules of the program to assure trademark and enforcement integrity and to avoid fraudulent declarations of compliance.

25. *Section 312.10(b)(2) requires that, in order to be approved by the Commission, self-regulatory guidelines include an effective, mandatory mechanism for the independent assessment of subject operators' compliance with the guidelines. Section 312.10(b)(2) lists several examples of such mechanisms. What other mechanisms exist that would provide similarly effective and independent compliance assessment?*

Section 312.10(b)(2) requires that a "mandatory mechanism" be used to conduct an assessment of compliance with self-regulatory guidelines, provides alternatives for achieving compliance, and is interpreted by commentary as precluding "self-assessment" as the only method for assessing operator compliance. As a starting point, we assume that the phrase "mandatory mechanism" means that all subject operators will be reviewed in accordance with the mechanism's assessment criteria and guidelines.

While we applaud the flexibility in the use of a combination of the three "mandatory mechanisms" proposed by the Commission, we believe that additional clarification with regard to compliance review activities be provided. For example, we recommend that compliance review activities be undertaken in two separate stages – an initial review and subsequent periodic reviews -- and that each be recognized by the regulations as separate and important components.

For example, both BBB*OnLine* and CARU currently conduct initial comprehensive reviews of eligibility of entities contending to be subject operators. BBB*OnLine* refers to these initial reviews, done prior to award or display of a compliance acknowledgment or seal, as compliance assessments. Similarly, when CARU is contacted by an operator to review its information practices, or when CARU finds a site that is not in compliance with its Self Regulatory Guidelines, CARU conducts a review of the site's information collection and privacy practices. Such initial reviews should be required by the Commission to encompass not only a comprehensive review of the operator's privacy policy, but should also reasonably ascertain that internal management controls and data collection, storage, security and use procedures are in place to make compliance with the privacy policy likely. Consumer reliance on an operator's alleged conformity to self-regulation guidelines cannot await ex post facto "periodic review" as the exclusive method for verification. In addition, the regulations should require additional initial assessments whenever an operator's policy or information practices are substantially changed or the operator's corporate organization relevant to data collection and use is substantially changed. In sum, in addition to the three mechanisms presented by the Commission, we believe that the first mechanism that should be employed by an

independent body is a review of the subject operator's practices in order to determine its initial compliance with the self regulatory guidelines.

Second, we agree that the subsequent "periodic reviews" of continued compliance are indeed crucial and appropriate requirements of the regulations. BBB*OnLine* conducts post-eligibility reviews in two ways-- on an annual basis all seal participants must complete an updated compliance assessment document, which BBB*OnLine* will review; and, in addition, all seal participants are subject to random and on-site verification reviews. CARU concurs that such periodic review is necessary not only when an operator adds new interactive features that may require changes to its privacy policy, but also at regularly defined intervals. We believe further clarification is needed, however.

For example, it would be helpful to clarify that the information practices referenced are only those practices required by the rule, rather than the full range of information practices in which the operator is engaged. In addition, while we agree that it would not be useful to provide a rigid definition of "periodic," we believe that the program's guidelines should be required to specify criteria, schedules or procedures for determining the timing of regularly conducted reviews. This might be "every six months," "every year," or "no less than every two years," or might vary depending on complaint history, changes made in site content and features, etc. Such a requirement would allow the public and the Commission to ascertain whether reviews are likely to occur as indicated and to compare the merits of different verification regimes.

Further, we interpret the distinction between review of information practices on a "random" basis and review of "all" information practices to mean that "random" refers to a program's option to review compliance by subject operators with some, but not all, eligibility requirements at defined intervals. In other words, as many government agencies typically do in enforcing statutory requirements, statistically acceptable, random auditing tools would be used to maximize compliance and minimize routine and unnecessary costs. For example, BBB*OnLine* expects to verify, with the assistance of outside experts,

different eligibility requirements for different operators, depending on criteria that are being devised to provide a high confidence level that the frequency and nature of reviews will be a reliable basis for assuming overall compliance. If our understanding of the distinction drawn between "random" reviews and reviews of "all" information practices is not correct we would appreciate clarification.

We also recommend that the regulations require that self-regulatory guidelines also require that if the random review option is selected, additional reviews will be made of other eligibility requirements if the random review indicates substantial non-compliance with the reviewed characteristics.

The Commission also suggests that seeding of a subject operator's databases in conjunction with periodic reviews is an effective mechanism to test compliance. CARU currently "seeds" many sites that have already been reviewed and found to be in compliance in order to help ensure continued compliance when new features are added to a site.

Finally, while we agree with the Commission's conclusion that assessment must not be based solely on self-assessment by subject operators, we believe that self-assessment can play an important role in ensuring that the subject operator's overall information and privacy practices are coordinated in a secure and effective manner. For example, where an operator has designated an information officer who is ultimately responsible for overseeing how data is collected or maintained and that a site is secure through the use of firewalls and encryption, etc., that officer could be responsible for supplying the self-regulatory body with a regular report or affidavit assuring compliance. Such an annual declaration could include a statement describing the operator's security
policies, processes, and procedures; or certify that it observes procedures consistent with our prescribed systems security rules. Under the Communications Act of 1934, such affidavits have been used as a method for telecommunications carriers to ensure the integrity of telephone communications from arbitrary or unauthorized eavesdropping or wiretapping.

26. *Section 312.10(b)(3) requires that, in order to be approved by the Commission, self-regulatory guidelines include effective incentives for compliance with the guidelines. Section 312.10Ib)(3) lists several examples of such incentives. What other incentives exist that would be similarly effective?*

The listed optional incentives for compliance with self-regulatory guidelines, include (i) mandatory, public reporting of disciplinary action taken against subject operators by the industry group promulgating the guidelines; (ii) consumer redress; (iii) voluntary payments to the United States Treasury in connection with an industry-directed program for violators of the guidelines; or (iv) referral to the Commission of operators who engage in a pattern or practice of violating the guidelines. While we believe the optional incentives for compliance are creative and helpful, they fail to distinguish among incentives that are useful options and those that are essential for adequate performance and public trust.

In our view, all safe harbor programs should be required to make referrals to the Commission in appropriate cases, and public reporting of disciplinary actions should be made in all cases, not merely as incentive options. For example, in the monthly NAD Case Reports, published by the National Advertising Division of the Council of Better Business Bureaus, CARU publishes formal cases against advertisers and site operators, as well as informal inquiries resulting in voluntary compliance or finding compliance, as well as work with operators or advertisers requesting pre-screening of their promotions to ensure regulatory compliance. BBB*OnLine* procedures similarly require the publication of all non-compliance findings and all dispute settlement decisions. Consumer redress and voluntary Treasury payments as optional incentives are useful, and perhaps could be evaluated by the marketplace when reviewing and comparing overall effectiveness of particular self-regulation programs, but they are not sufficient substitutes for referral and publicity incentives.

In this regard, we also recommend that Commission referrals should be required whenever there is a failure of the operator to bring practices into compliance when non-compliance is identified, without waiting for a "pattern or practice" of non-compliance to

develop. CARU and BBB*OnLine*, for example, will refer all cases of non-cooperation to the Commission, and indeed would not expect to have continuing violators remaining as supporters or program participants.

Finally, we urge an additional required incentive, namely mandatory corrective action consistent with the scope of the violation uncovered (e.g., "take Mrs. Jones off the mailing list," or "rewrite the company's onward transfer procedures").

Additional Recommended Safe Harbor Requirements

1. Insulation of Investor Influence from Decisions

We believe that self-regulation programs must not be influenced by investor profit motive. We urge that safe harbor status be available only to non-profit organizations or to for-profit companies that otherwise demonstrate that self-regulatory decisions are completely insulated from owner or investor influence or control. Cf. 16 CFR §703.3(b) [warrantor dispute settlement mechanisms must be "sufficiently insulated" from the warrantor]. The profit incentive should not be allowed to compromise compliance and dispute settlement activities.

2. Additional Incentives—"Prior Resort" and Civil Penalty Waiver

The proposed incentive regarding Commission consideration in cases of possible non-compliance by safe harbor program participants of whether to launch an investigation or of appropriate remedies are very helpful, but in our opinion do not go far enough.

An additional helpful incentive to participate in a safe harbor program would be an affirmative commitment by the Commission to refer in the first instance privacy complaints under the COPPA rule to safe harbor programs that offer accessible, affordable and timely dispute settlement procedures. This would be similar to the "prior resort" option for consumer product warrantors under 16 CFR §703.2. A similar "prior resort" incentive should also be applicable to State Attorney General actions otherwise authorized by

COPPA. Under this approach, complaints filed with the Commission or state and local authorities would be referred to the approved safe harbor program, and would not be processed by the public agency unless compliance were not achieved by the program in a reasonable time. As we envision such a requirement, the program would report the result of its review to the "referral" agency, which could proceed if non-compliance remains or if a pattern of non-compliance is demonstrated.

Similarly, because violations of Commission rules carry the risk of civil penalties, the Commission could further provide incentives for self-regulation by waiving civil penalties for operators that comply in good faith with the safe harbor program's directions for corrective action.

ADDITIONAL SAFE HARBOR COMMENTS

1. **§312.10(c)**

We understand and appreciate that the application material proposed to be required is probably designed to enable efficient and thorough review by the Commission and to allow the public to make meaningful comment on the application for safe harbor treatment. We are concerned, however, that the application requirements could unintentionally impose unnecessary burdens and result in a mechanistic application of the requirements to everyone's disadvantage.

We believe that the information required under (c)(i) and (ii), namely the full text of the guidelines and a comparison of each provision of the guidelines to the corresponding requirements of the Rule, should provide a sufficient basis for Commission action. Any further statement [as proposed in (c)(iii)] explaining how the guidelines, including the assessment mechanism and compliance incentives, meet the requirements of the Rule should be optional. In most cases the "match" of guidelines and Rule

requirements should speak for itself, and where further explanation is desired the applicant can be expected to provide it or not at its own peril. If our recommendation to make the (c)(iii) requirement optional is accepted, we recommend that (c)(i) be clarified to include reference to the assessment mechanism and compliance incentives, and that (c)(ii) be amended to add §312.10 to the list of Rules requiring comparison to the guidelines.

2. **§312.10(c)(2)**

COPPA affords the Commission 180 days to act on applications for approval of safe harbor guidelines. We also recognize that the Commission needs a reasonable time to make a thorough review and consider public comments. The fact remains, however, that six months is a huge time period to ask applicants and their participating companies to wait for approval and the attendant certainty.

We recommend that the Commission signal its intention to proceed with the urgency demanded by the subject, and provide in the Rule that it will normally determine applications within a 90-day period. Such a time frame might be temporized by allowing the Commission to determine in particular cases requiring additional time, and publish a notice to the effect, that additional time is needed on a particular application.

At the very least we recommend that in cases where further information is needed from the applicant that the Commission not restart the time clock unless the missing information precluded any meaningful review from being commenced. If additional information is requested, the decision-making time frame may be tolled, but should not be restarted, because of the unnecessary delay that restarting the clock would entail and its susceptibility to abuse. In this regard, if there is missing information that did not preclude the start of a meaningful review, the Commission should simply request the additional information, and not reject the application as suggested by the commentary to the proposed Rule.

Further, the Commission should specify the amount of time that generally will be afforded the public to comment, say 30 or 45 days. As the commentary now reads it appears that the time for comment will be set on an individual basis, which might not be fair to either the public or the applicants, and might subject the Commission to charges of bias.

Finally, the commentary provides that Commission approval of any application will be effective 45 days from publication in the Federal Register. Given the delays sometimes encountered by agencies in Federal Register publication, approvals might not become effective for as much as six weeks or more after actual agency action. We see no purpose to this delay. Unlike a rule that would impose a burden on a segment of the public, and which therefore might reasonably be delayed to provide opportunity for getting into compliance, safe harbor application approvals will provide a benefit and impose no hardships requiring planning or adjustment. Indeed, the extra period prior to effectiveness of the approval may well contravene the statutory requirement for final agency action within 180 days, at least in cases where the agency 's approval takes longer than 135 days to complete.

3. **§312.10(d)**

As proposed, the records provision of the Rule establishes a retention time period for consumer complaint records (three years), but none for records of disciplinary actions and independent assessments. This suggests that these records will need to be maintained permanently. We do not understand why this is needed, and recommend that a uniform record retention standard be adopted. Three years, or for so long as the operator remains a participant, whichever is longer, seems appropriate. In addition, we urge the Commission to consider whether and to what extent maintenance of records in electronic form can satisfy the Rule.

Finally, it is crucial to the success of self-regulation programs that proprietary data that is submitted by applicants or is referenced in assessment and verification reviews by the self-regulation program retain the confidential status they are afforded by the program as a means to encourage voluntary participation. At the very least, these materials should be afforded trade secret status under the Freedom of Information Act, which would allow for notice to the company that a request for the proprietary information has been made.

****

Again, we congratulate the Commission for its appreciation and understanding of the twin goals of protection of children's online privacy and of encouraging the private sector to create the programs needed for effective implementation these protections. CBBB, its two divisions, CARU and BBB*OnLine*, and our supporters, sponsors and participants, will continue to work closely with the Commission and its staff to ensure effective implementation of COPPA and maximum, safe enjoyment of the Internet by children.

Respectfully submitted,

Elizabeth Lascoutx, CBBB Vice President and Director, CARU

elascoutx@caru.bbb.org

A. Cassidy Sehgal, CARU Staff Attorney

csehgal@caru.bbb.org

Gary Laden, Director, BBB*OnLine* Privacy Program

gladen@cbbb.bbb.org

Shea Hickman, BBB*OnLine* Privacy Program Compliance Specialist

shickman@cbbb.bbb.org

Steven J. Cole

CBBB Senior Vice President and General Counsel

scole@cbbb.bbb.org

Enclosures