CENTER FOR MEDIA EDUCATION
2120 L Street, NW, Suite 200
Washington, DC 20037

1424 16th Street, NW, Suite 604
Washington, DC 20036

June 11, 1999

Donald S. Clark
Secretary
Federal Trade Commission
Room H-159, 600 Pennsylvania Avenue, NW
Washington, DC 20580

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

Dear Mr. Clark:

The Center for Media Education, the Consumer Federation of America, American Academy of Child and Adolescent Psychiatry, American Academy of Pediatrics, Junkbusters Corporation, National Alliance for Non-violent Programming, National Association of Elementary School Principals, National Consumers League, National Education Association, Privacy Times and Public Advocacy for Kids (hereinafter "CME/CFA, et al.") respectfully submit these comments in response to the Federal Trade Commission's ("FTC" or "Commission") proposed rule implementing the Children's Online Privacy Protection Act (hereinafter "COPPA" or "the

Act") Notice of Proposed Rulemaking to Implement the Children's Online Privacy Protection Act of 1998, and Proposed Rule, 64 Fed. Reg. 80, available at http://www.ftc.gov/os/1999/9904/index.htm (April 27, 1999) ("NPRM"). CME/CFA, et al. include a broad coalition of child advocacy, education, health and parents groups dedicated to improving the quality of electronic media, especially on behalf of children and their families.[1] For three years, we have urged the FTC to develop safeguards for protecting children online. CME/CFA, et al. look forward to this process culminating with a set of rules capable of effectively protecting children's privacy.

Senator Bryan, who co-sponsored the Act with Senator McCain, noted that Congress enacted COPPA to protect children online. Specifically, Senator Bryan stated,

> The goals of this legislation are:
> (1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in an online environment;
> (2) to enhance parental involvement to help protect the safety of children in online fora such as chatrooms, home pages, and pen-pal services where children may make public postings of identifying information;
> (3) to maintain the security of personally identifiable information of children collected online; and
> (4) to protect children's privacy by limiting the collection of personal information from children without parental consent.

Cong. Rec. S11657 (daily ed. Oct. 7, 1998) (statement of Sen. Bryan). The Act does not contemplate that the FTC engage in any balancing of the interests of children and the interests of industry, nor does it suggest that the FTC should take any action that facilitates information

[1] See Appendix A for a description of each of the organizations supporting these comments.

collection from children. Thus, the FTC's mandate is clear. It must implement the Act in a way that best protects children's interests.

In these comments, CME/CFA, et al. will first discuss several provisions in the proposed rules that the Commission did not address in its specific questions. Much of this discussion includes attempts to clarify language which could be easily misinterpreted in order to ensure that the Commission's rules will serve the goals of the Act. CME/CFA, et al. are particularly concerned about the FTC's definition of operators and third parties and the responsibilities that attach to these entities. As we describe in more detail, infra, third parties must be required to comply with the FTC's rule. The FTC should not permit the disclosure of information to third parties in such a way that undermines the intent of the legislation. Following this discussion, we offer our responses to the specific questions posed by the Commission.

General Question

---

1. Please provide comment on any or all of the provisions in the proposed Rule. For 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.

§312.2 DEFINITIONS

Collects or collection

CME/CFA, et al. support the Commission's inclusion of passive tracking and the use of cookies, within the definition of "collection."[2] This provision will prevent operators from circumventing COPPA's intent by surreptitiously gathering information in a passive manner and

---

[2] NPRM at 6.

later connecting it with personal information. CME/CFA, et al. also agree with the Commission that collection includes all online requests regardless of whether the transmission of information in response to that request is online or offline.[3]

In addition, CME/CFA, et al. believe that the FTC should consider the combination of information gathered from offline sources with information collected online as a form of collection under the rule. Without this provision, information vendors could collect information from a child through traditional offline methods, e.g., through forms on cereal boxes, and provide this information to operators for the purposes of marketing to the child online. Under the proposed rule, if the child's information was not requested online, the partnership between the information vendor and the operator would not invoke any operator responsibilities, and a parent would have no way of knowing that information about her child was being used by an operator. To ensure that the goals of COPPA are achieved, the FTC should modify its rules to encompass these business practices.

Furthermore, the FTC's definition of collection should include any acquisition of information by an operator of a Web site which is directed at children even if the information is gathered from another Web site which is not directed at children. For example, ESPN.com should not be permitted to share information freely with its Go Network affiliate Disney.com because the latter is an operator of a Web site directed at children. If an individual registers with the Go Network through ESPN.com and then attempts to access the Disney.com Web site, Disney.com should be considered to be collecting information, even if it is collecting the data

[3] Id.

from ESPN.com or the Go Network, rather than from the child while he was on the Disney.com portion of the network.[4]

Similarly, the collection of children's information by third parties from operators should be considered a form of data collection subject to this rule. Defining "collection" in this manner would place responsibilities on third parties to protect children's privacy. Without such protections, children's privacy protections could be easily circumvented by operators who could transfer information to third parties capable of using that information on the operators' behalf. For example, an operator could adopt seemingly comprehensive privacy practices to lull a parent into a state of complacency. After acquiring the parent's trust, the operator could request to release some information to a third party, which could be a subsidiary or partner of the operator. Under the proposed rule, the third party's use of the information would be virtually unrestricted. If the third party were a subsidiary or partner of the operator, the operator could easily access children's information without adhering to its own more restrictive privacy policies.

Disclosure

The Commission should specify that contractors who provide technical support or fulfillment services will be exempted from the definition of disclosure only if they do not use or maintain any information about the child beyond that which is necessary for them to perform their technical support or fulfillment services and if they delete that information as soon as its retention is no longer necessary. The Commission should also clarify that the two clauses (a) and (b) in the

[4] CME/CFA, et al. does not intend to criticize the privacy practices of ESPN.com, Disney.com, or the Go Network. These Web sites are being used as examples solely due to their unique structure which incorporates a number of popular Web sites, including some directed at children, into a single network with, at least potentially, a single registration scheme.

definition of disclosure are each independently sufficient to define a form of disclosure.[5] The definition is currently ambiguous, and should be clarified by replacing the word "and" between these clauses with the word "or".

Third Party

The Commission should elaborate on its definitions of operators and third parties under the proposed rule to clarify that all entities with access to information collected from children must comply with the FTC's rule.[6] Moreover, the category of operators should also include any agents of the operators.[7] If the FTC considers a party to be an operator only if it collects information directly from the Web site, then, under the proposed rule, an operator may easily transfer the information it collected from children to other entities which may not be limited by the same restrictions as operators.[8]

Online Contact Information

Under the proposed rule, online contact information is an identifier that permits direct online contact with a person.[9] The definition of online contact information should include identifiers held in persistent cookies if those identifiers permit individual contact. For example, a Web site may identify and individually address a child, by welcoming him by name, based upon

---

[5] NPRM at 6.

[6] NPRM at 7.

[7] See question 3, infra, regarding the definition of "Operator" for a more detailed discussion of CME/CFA, et al.'s views on the operator/third party distinction.

[8] While the rule provides parents with an opportunity to limit this transfer by denying consent to third party disclosure, many parents may fail to do so because they will expect third parties to follow the same information practices as the operator.

[9] NPRM at 7.

information stored in cookies. In such cases, the information stored in the cookies should be considered online contact information.

Web site or Online Service Directed to Children

CME/CFA, et al. support the Commission's decision to consider highly contextual cues such as evidence regarding the intended audience and the use of activities and incentives which appeal to children to determine whether a Web site or online service is directed to children.[10] As the FTC states, an operator of a general interest Web site or online service will have duties under the proposed rule if it knows that a particular visitor is a child.[11] CME/CFA, et al. believe that operators who ask visitors their age should be required to include "under 13" as an option. A user's selection of this option should trigger responsibilities for the Web site operator under the rule. Operators should not be permitted to construct a veil of ignorance for themselves by including both teenagers and children in their youngest age category, e.g., by creating a "15 and under" category.

The Commission should better protect children by expanding what it means to have a "portion" of a Web site or online service directed at children. This definition should include clearly labeled children's pages within a Web site, as well as pages which include specific requests for information directed at children whether or not they are located in a section of the Web site designated as targeting children. For example, a baseball page which takes polls of its users might not be directed to any particular age group. If, however, the poll asks the user whether he currently plays in Little League, then any page linking to that question should be considered a

[10] Id.
[11] Id. at 11.

portion of the Web site directed at children, and the Web site's operator should be responsible for adhering to the FTC's rules. Additionally, the section on which the question appears should also be considered to be directed at children.

Similarly, a "portion" of a Web site or online service should include entire Web sites directed at children within a larger registration structure, even if that larger structure includes Web sites not directed at children. For example, the Go Network currently includes both ESPN.com and Disney.com. If a child registers with the Go Network through ESPN.com, she will be outside of the scope of this rule because ESPN.com is not directed at children. If the child then accesses the Disney.com site, Disney.com could circumvent the FTC's rules and gain information about the child through her Go Network registration. To prevent operators from evading their responsibilities, the rules should define a "portion directed at children" to include entire sites within a larger registration structure, as well as specific requests for information about a child regardless of whether the request is directed to the child, an affiliate (ESPN.com), or a larger network (Go). In this example, the user's accessing of the Disney.com site should be considered a triggering event, i.e., a specific request for information directed at children which should notify ESPN.com (and other Go affiliates) that this user might be a child, in which case information cannot be collected from her without parental consent.[12]

[12] Similarly, if a child registers with Disney.com with her parent's consent, Disney.com's Go Network affiliates should be on notice that the registrant is a child, and they should not have access to that child's information without obtaining additional verifiable parental consent.

§312.3 UNFAIR AND DECEPTIVE ACTS AND PRACTICES

General Requirements

As currently drafted, the general requirements in the proposed rules appear to apply only to operators and not third parties.[13] The rule should be clarified to indicate that these requirements extend to third parties as well. Exempting third parties from these requirements would permit operators to avoid complying with the rules by partnering with third parties who can use children's information on the operators' behalf.

§312.4 NOTICE TO PARENTS

§312.4 (a) General principles of notice

The rule should require that notice be provided in a format that will be easy for parents to understand. If multiple operators are providing notice, the Commission should require them to agree upon a single policy with respect to children's information. In the alternative, the operators should have joint responsibility to furnish a single notice which compiles their policies in a format which is both comprehensive and simple.

§312.4 (b) Notice on the Web site or online service

§312.4 (b) (1) Placement of the notice

Under the Commission's proposed rule, when there are multiple sets of practices or policies on the same Web site, operators must label these different practices clearly and write them in such a way as to avoid any confusion.[14] CME/CFA, et al. suggest that the Commission require multiple operators to agree to a single information collection and use policy for each Web

[13] NPRM at 11.
[14] Id. at n.9.

site. If the Commission decides not to adopt such a requirement, it should adopt a high standard to ensure that multiple operators on a single site present their collection policies in a simple and clear manner.

§312.4 (b) (2) Content of the notice

In its explanation of parental notification requirements, the Commission states that notice must include "(f) what general measures the operator takes to ensure the confidentiality, integrity, and quality of the information collected."[15] The FTC omitted this provision from the text of the proposed rule. The rules should be revised to include this provision.

§312.4 (b) (2) (ii)

The FTC should emphasize the importance of listing the specific types of information collected. The Commission notes that the statement, "[w]e collect personal information from your kids" is an insufficient disclosure.[16] However, the FTC's explanation is slightly misleading because it implies that any disclosure more specific than this general statement would be acceptable. The Commission should clarify that the rule requires operators to describe the specific types of information collected.

The rule also states that parents should be notified whether personal information is collected directly or passively.[17] Operators must inform parents of their collection methods in a meaningful manner. Because most parents will be unfamiliar with terms like "passive collection," operators should describe their collection methods in terms that are easily understood, such as "We track your child's use of our site via cookie technology built into their web browsers. This

[15] Id. at 14.
[16] Id. at 15.
[17] Id. at 14.

practice allows us to determine which areas of our Web site they have visited as well as the time, date, and frequency of their visits to each of those areas."

§312.4 (b) (2) (iv) Third party disclosure

In addition to requiring Web sites or online services to inform parents about the types of business in which third parties are engaged, the FTC should also require the sites or services to provide parents with the names of those third parties and their contact information. The FTC should require that third parties maintain the same privacy policies as the operator. However, if the FTC does not adopt this suggestion, the FTC should mandate that the operator clearly state how the policies differ, especially if the third party's policies are less stringent. In addition, operators should be required to inform parents how they can prohibit the disclosure of information to third parties.

§312.4 (b) (2) (v)

The Commission should construe narrowly the reasonableness standard in the proposed rule when determining whether a request for information is reasonably necessary.[18] Operators who create reasons for collecting information (such as sending a "thank you" e-mail to a child who plays a game online and, thus, collecting that child's e-mail address) should be seen as acting unreasonably. The Commission should consider it a deceptive trade practice for an operator to suggest that a request for information is necessary if the necessity is contrived.

§312.4 (b) (2) (vi)

The rule should require that the procedures by which a parent "can review, make changes to, or have deleted the child's personal information" be clear and simple.

---

[18] Id. at 16.

§312.4 (c) Notice to a parent

Under this section, the FTC allows operators to use forms of notice that may never be seen by a parent. The FTC should require operators to take additional steps to make parental receipt of notice more likely. We discuss some of these options in our response to question 9, infra.

In addition, the Commission should adopt rules requiring that notice to parents be sent in a timely fashion. The operator should send notice to the parent as soon as it collects the parent's contact information.

§312.4 (c) (1) Content of the notice to the parent

The notice should also include the fact that parents have the option of denying consent for information collection from their child.

§312.4 (c) (1) (iii) (A)

When providing notice under the exception described in §312.5(c)(3), the operator should inform the parent how often and with what frequency it plans to contact the child.

§312.4 (c) (1) (iii) (B)

The rule should specify that a parent retains his right to refuse to permit further contact with his child and can exercise that right at any time. The notice should include simple instructions explaining how a parent can prohibit further contact with his child.

§312.4 (c) (1) (iii) (c)

The rule should clearly state that a later revocation of consent or a decision to "opt-out" constitutes a response to the notice. Operators should be required to immediately process all revocations of consent and opt-outs.

§312.5 PARENTAL CONSENT

§312.5 (a) General requirements

§312.5 (a) (1)

CME/CFA, et al. strongly support the Commission's decision to require operators to obtain verifiable parental consent before they can use information previously collected from children for purposes not initially consented to by their parents.[19] Without this provision, children who had the opportunity to participate in online activities before COPPA would be denied the same privacy protections as new users. In addition, unscrupulous operators could claim that newly collected children's information was collected before the enactment of the rule, making enforcement of COPPA difficult.

CME/CFA, et al. also support the Commission's decision to require operators to re-obtain verifiable parental consent each time they change their information collection practices. However, CME/CFA, et al. are concerned about the potential for parents to be unnecessarily badgered by frequent changes in privacy practices. Thus, CME/CFA, et al. suggest that the Commission consider adopting measures to limit the number of such changes by operators.

§312.5 (a) (2)

At the same time that the operator provides the parent with the option of consenting to collection and use of a child's information, the parent must be offered the option of denying consent to the disclosure of that information to third parties. The method of limiting consent must be clear and simple.

---

[19] NPRM at 19.

§312.5 (b) Mechanisms for verifiable parental consent

The FTC should require that operators retain records of parents' consent, regardless of which particular method of gaining consent the operators use. These records will provide verifiable evidence of parental consent as required by COPPA. In addition, the FTC or any agent charged with assessment of the Web site or online service under the safe harbor rules can rely on these records when reviewing operators' practices.

The Commission should also note that a toll-free telephone number is insufficient on its own if it is automated or handled by untrained telephone operators. Consent through a toll-free telephone number would be verifiable only if that number is answered by trained personnel who can determine whether a caller is actually a parent.

§312.5 (c) Exceptions to prior parental consent

CME/CFA, et al. support the Commission's recommendation that operators voluntarily delete all information collected as soon as it is no longer necessary to retain that information.[20] In addition, the Commission should require that the notice to parents clearly provide them with the option of opting out of further information collection, even when prior parental consent is not required.

§312.5 (c) (2)

The FTC should limit this exception to instances in which the operator specifically responds to an individual user's request. Requests which consist of clicking on a button to receive generic information via e-mail are not specific. CME/CFA, et al. support the

[20] Id. at 21.

Commission's suggestion that commonly requested information be posted directly on the operator's Web site rather than be sent via e-mail to children.

§312.5 (c)(3)

CME/CFA, et al. support the Commission's recommendation that operators collect parents' e-mail addresses instead of children's contact information, while providing parents with the option to substitute their children's addresses.[21] In addition, the FTC should require that any notice provided to the parent under this exception include information about the nature of the contact with the child, including the subject, purposes, and frequency of that contact. Both the notice and each instance of communication (such as a newsletter) sent to the child should also include an explanation of an easy means for parents to request that operators discontinue any contact with their children.

The Commission should recognize that its suggested methods of providing notice will not ensure that a parent actually receives that notice.[22] An e-mail message sent to an address a child identifies as a parent's e-mail address may never be received by the parent. Whether by design or accident, the e-mail might be intercepted by the child (or a friend of the child) or sent to a third-party unknown to either the child or parent. To ensure that a parent received an e-mail, the operator should request confirmation from the parent. If no confirmation is received and the operator already has the parent's mailing address, the operator should send the parent notice by postal mail with a business reply card which the parent can return to confirm receipt of the notice.

[21] Id.
[22] See id. at 21-22.

§312.6 RIGHT OF PARENT TO REVIEW PERSONAL INFORMATION PROVIDED BY CHILD

§312.6 (a)

The Commission should require operators to provide parents with the option of directly requesting the specific information collected from their child. The Commission's two-tiered approach is excessively cumbersome for those parents who wish to see the specific information.[23] If the Commission allows a two-tiered approach, it should require the operator to provide clear and prominent instructions which explain how to request access to specific information.

§312.6 (b)

Operators should be penalized if they do not take steps to ensure that the person to whom a child's information is disclosed is the parent of that child. Moreover, reasonable procedures for disclosure must include a process to deal with the unavailability of the consenting parent as a result of death, desertion, or divorce.

§312.6 (c)

CME/CFA, et al. support the Commission's position that, even if parents refuse operators' requests for consent to collect information from their children, operators should allow these children to participate in any activities which do not require that information.[24] In addition, the operator should disclose in the notice what information is necessary for the specific activities (or types of activities) in which their children might seek to participate. This notification will permit parents to make informed decisions about the value of the activities in which their children may participate and the desirability of permitting the release of their children's information.

---

[23] See id. at 23-24.
[24] Id. at 26.

§312.8 CONFIDENTIALITY, SECURITY, AND INTEGRITY OF PERSONAL INFORMATION COLLECTED FROM CHILDREN

This provision should include a requirement that operators exercise due care when dealing with third parties. For instance, an operator should review third parties' business practices before disclosing any information to them. If an operator acts irresponsibly (for example, by dealing with a third party it has reason to suspect will lie about its information practices), the operator should be held accountable for its negligence.

§312.10 SAFE HARBORS

§312.10 (d) Records

The FTC should require that operators seeking safe harbor treatment maintain records of parental consent including information about the reason and extent of the consent, the method used to grant consent, and the date of each instance of consent.

§312.11 RULEMAKING REVIEW

Given the ever-changing nature of the Internet and online technology, CME/CFA, et al. suggest that the FTC review its rulemaking in three years rather than five years. The Commission should also review the efficacy of the safe harbor provisions when reviewing the implementation of the rule.

Definitions

2. Section 312.2 defines "Internet." Is this definition sufficiently flexible to account for changes in technology? If not, how should it be revised?

The definition of Internet should be clarified so that it clearly includes networks parallel or supplementary to the Internet such as those maintained by the broadband providers @Home and RoadRunner. It should also include intranets maintained by online services which are either accessible via the Internet or have gateways to the Internet.

In addition to defining "Internet," §312.2 should also define "online services." Online services should include any interactive service provided over a network, including online information services such as Lexis-Nexis, electronic bulletin-board systems which are not connected to the Internet, and interactive digital television.

The Commission's implementation of COPPA should not override any stricter existing laws governing other media, e.g., cable privacy rules.

3. Section 312.2 defines "operator."
(a) Is this definition sufficiently clear to provide notice as to who is covered by the Rule?

As stated earlier, the FTC should clarify the definitions of operators and third parties. For example, the FTC should clarify that subsidiaries of operators, for the purposes of the rule, are considered operators themselves. Thus, each subsidiary of an operator that has access to information collected from children must obtain separate consent from parents. In addition, the FTC should expressly define an entity as an operator once such an entity receives information through the Internet or relevant online service or once that entity acquires the legal right to use the information.

The Commission indicates in its explanation of the definition of "operator" that it intends to demonstrate some flexibility in determining who is an operator, taking into account "such

factors as who owns the information, who controls the information, who pays for the collection or maintenance of the information, the pre-existing contractual relationships surrounding the collection or maintenance of the information, and the role of the Web site or online service in collecting and/or maintaining the information."[25] The FTC should treat each of these factors, if satisfied, as sufficient for a determination that an entity is an operator. Thus, for example, operators should not escape responsibility because they control the information but do not pay for its collection or maintenance.

(b) What is the impact of defining the term in this way?

CME/CFA, et al. generally support the Commission's decision to define operators in terms of their relationship to information collected. The FTC's definition recognizes that more than one entity may be capable of accessing or controlling information gained from a single Web site, and it allows all such entities to be defined as operators. Under the rule, each operator who collects information from a child is separately responsible for safeguarding that information, thus providing additional layers of protection for children. To minimize confusion for parents, CME/CFA, et al. strongly suggest that the Commission require multiple operators who collect information from a single Web site to maintain a single, unified set of information practices.

However, if the FTC allows multiple operators using a single Web site or online service to use multiple information practices, it should clarify whether multiple operators should obtain consent or grant access individually or cooperatively. CME/CFA, et al. believe that multiple information practices might be confusing for parents, while a unified information practice may encourage the sharing of information between operators, some of whom may be operators for

[25] Id. at 8.

multiple Web sites. When there are multiple operators, a Web site should include a single interface and/or contact for parents who will distribute information to the various operators. Each operator can then individually contact parents without sharing information with other operators. This method will limit any confusion on the part of parents while restricting the ability of operators to share information illicitly.

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 messaging user identifier; a screen name that reveals an 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 consider adding to this list?

The Commission should specify that it has the authority to determine in the future that other identifiers could be considered personal information. CME/CFA, et al. believe that any information (whether collected online or offline) which is linked to personal information should itself be considered personal information. For example, if any information (which would not otherwise be considered personal information) is collected online and linked to personal information collected from offline sources, that information should be considered personal information under the rule.

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?

Notice should be unavoidable, prominent, and clear. Any link to notice should be compelling to both parents and children and should not be labeled in a manner which belittles the importance of privacy. Some Web sites undermine their privacy policies by presenting them in an unappealing way.[26] For example, Kellogg's Cereal City displays a link to its privacy policy in a prominent location, but treats it differently from other links on the page which have colorful icons and explanations.[27] Similarly, in the "Time for Kids" section on pathfinder.com, the privacy policy is in a small font at the bottom of the page, so that users must scroll down to reach it.[28]

The proposed rule notes that typical visitors to a Web site should be able to see the link without scrolling. If the Web site includes internal anchors allowing a visitor to enter the home page at a point other than the top, the Web site should have a link to the privacy policy available at that point without the need to scroll up or down. Access to notice should also be available continuously from a variety of points within the Web site at a static location which parents can bookmark if they so desire. In particular, notices should be available whenever consent is requested and whenever an operator seeks to collect a new type of information. Thus, the

---

[26] See also, CME/CFA, et al.'s response to question 5(b) for a discussion of the types of language that should and should not be used by Web sites.

[27] See Kellogg's Cereal City (visited May 11, 1999) <http://www.kelloggs.com/index_cc.html>.

[28] See Time for Kids (visited May 11, 1999) <http://pathfinder.com/ TFK/index.html> .

Commission should take action against Web sites that do not present links to their privacy policies on their registration page.[29]

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

As the Commission notes, labeling a link to policies concerning information practices as "About Us" or "What We Do" is insufficient.[30] Instead, links should be labeled in a more salient manner, such as "Privacy Policy" or "What We Do With Information You Give Us." The content of the policies should be understandable and compelling according to a reasonable child standard.[31] Thus, the notice should emphasize the importance of privacy using simple, non-legalistic language that both parents and children can understand. The Commission should stress that language undermining the importance of privacy policies, such as labels stating "Our lawyers made us say this," are unacceptable.[32]

6. Section 312.4(b)(2)(I) requires the notice on the Web site or online service to state the name, address, phone number, and e-mail address of all operators collecting personal information through the Web site. Where there are multiple operators collecting personal

---

[29] See, e.g., Curiocity's Freezone (visited May 11, 1999) <http://www.freezone.com>.

[30] NPRM at n.8. See also Yak's Corner (visited May 11, 1999) <http://www.yakscorner.com>(labeling their privacy policy uninformatively as "Teachers/Parents").

[31] The Commission has recognized the need for a special reasonableness standard for children. In its FTC Policy Statement on Deception, the Commission notes that the existence of a special reasonableness standard will depend upon the context of the deceptive practice. The Supreme Court has affirmed this approach, stating that the "determination whether an advertisement is misleading requires consideration of the legal sophistication of its audience." Bates v. Arizona, 433 U.S. 350, 383 n.37 (1977).

[32] For example, the Jelly Belly Web site's legal page is subtitled "Information only Mr. Jelly Belly's lawyer would love" and there is no indication in either the link to the page or the title of the page that the Web site's privacy policy is located on this page. This language should be considered inappropriate. See Jelly Belly Legal Stuff (visited May 10, 1999) <http://www.jellybelly.com/legal.html> .

information through the Web site, are there other efficient means of providing information about the operators that the Commission should consider?

All operators collecting information must be listed with contact information. Parents should have the ability to contact any operator possessing information about their children. However, as previously stated, CME/CFA, et al. maintain that multiple operators could choose a single contact operator who would be responsible for distributing parental queries in an appropriate manner. Parents need easy access to information about operators, and the FTC should facilitate parents' access regardless of the burden on the operators. If operators find complying with notice requirements too burdensome, then they should refrain from collecting information from children.

7. Section 312.4(b)(2)(iv) requires an operator to state whether the 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?

The Commission should not permit operators to disclose information to third parties unless those third parties comply with this rule. Operators should provide parents with detailed information about the third parties' intended use of the collected information. Operators should also inform parents about the third parties' specific disclosure, confidentiality, integrity, and security practices. CME/CFA, et al. ask the Commission to require operators to disclose information to third parties only if they have the same collection and use practices as the operator. However, if the Commission allows operators to disclose information to third parties with less stringent privacy practices, the operator should be required to inform parents of this fact. An operators should emphasize any standards or policies that a third party adheres to which are less stringent than the operator's practices. Without such information, parents will be unable to

make informed decisions about whether to allow information to be shared with third parties. Most parents may likely assume that third parties use the same privacy practices as operators.

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)?

CME/CFA, et al. support the Commission's decision to require that notice be provided directly to parents as well as on the operator's Web site or online service. While COPPA requires that parents receive the notice directly, posting it on the Web site allows parents continued access to the information. In addition, an archive of past notices should be available on the Web site or online service, so that parents can review any changes which may have been made in the information practices of an operator or third party. This archive should always be available through an appropriately-labeled link directly from the current notice.

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?

As discussed supra in our response to question 1, the Commission's proposed methods of providing notice may not be effective. The FTC should raise the standard for notice to ensure that it is received. For example, if notice is sent by postal mail, operators could include a business reply mail postcard for parents to send back indicating their receipt of the notice. If notice is sent by e-mail, parents could confirm receipt by replying to the operator. While neither of these notification methods would qualify as verifiable parental consent, they increase the likelihood that parents will actually receive the notices sent.

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?

All of this information is necessary. Parents need detailed notice to appreciate how their children's information is being used and disseminated. They also must be informed of their rights to limit the use and dissemination of the information.

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

The FTC should require operators to explain how parents can refuse or limit further contact with their child. Without such a requirement, a parent's right to control her child's information may be meaningless, especially if she is faced with a recalcitrant operator.

The operator should also notify the parent if its practices fall within a "safe harbor," and, if so, the operator should provide information on how to report violations of the safe harbor guidelines. The notice should include all rights to redress available if the operator violates its privacy policy, regardless of whether or not the operator falls within safe harbor protection.

Parental Consent

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.

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

This formulation is not excessively burdensome. The operator must ensure that parents have a means of contacting all parties who hold their children's information. If operators who are involved in mergers or corporate combinations find it too burdensome to comply with the Commission's rules after their mergers, they should no longer use the collected information.

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

The FTC should place the same obligations on operators and third parties. Such a provision would relieve operators of some policing duties, and allow them to share responsibility with those third parties who benefit from the disclosure of children's information. The FTC must also require that parents receive contact information for third parties.

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?

Yes. Parents should be given the option to refuse consent to different internal uses of information. For example, a parent should be allowed to permit an operator to use a child's information in aggregate form in order to improve its services, but deny the operator the right to contact a child by e-mail or target a child with personalized advertisements. Meaningful implementation of this provision would enhance parents' control over their children's information, and would reduce the risk of an operator deceiving a parent into consenting to an inappropriate

use of a child's information. If parents do not have the right to consent selectively, operators could hide an inappropriate use of children's information within a long list of unobjectionable uses. Parents would be less likely to consent to an inappropriate use if they had to grant consent to each use individually.

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?

Yes. Parents have successfully used most of these methods (with the exception of e-mail-based mechanisms such as digital signatures), offline for many years in a variety of situations. For example, parents commonly sign printed permission slips to enable their children to participate in school activities.

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

The most obvious benefit of the listed methods is that they meet the Congressional mandate of verifiability, increasing the certainty that parents will be able to regulate the disclosure of information about their children. Parents have a fundamental right to protect their children from commercial contact and exploitation. In addition, parental involvement is necessary to curb the impulsiveness of children and to help compensate for their children's naivete. Without verifiable methods of consent, parental involvement cannot be guaranteed.

Implementing these verifiable methods for consent would minimize the likelihood that children would circumvent the process. In contrast, children could easily circumvent e-mail-based consent methods which do not utilize digital signatures or other similar verification mechanisms. Children often share their parents' e-mail addresses and can easily intercept, even inadvertently,

requests for parental consent. Moreover, even if children have their own e-mail accounts, they can typically enter any e-mail address as their parent's, allowing them to redirect requests for consent to their own e-mail account or to the account of one of their friends.

Current e-mail-based consent procedures include automated methods of gaining consent. For example, some Web sites include a hyperlink within the e-mail message to the parent. Clicking on the link immediately registers the child at the site.[33] While such processes may be economical for operators,[34] any increased costs of non-automated methods will be temporary because digital signatures and other verifiable electronic mechanisms will soon come into common use.[35] However, verifiable electronic methods of consent are not yet available. The current e-mail based systems are not verifiable and do not meet the Congressional mandate in the Act.

In performing any cost/benefit analyses of the different methods of verifying consent, the Commission must consider that operators derive financial benefits from collecting information from children regardless of the consent method used. Moreover, children, parents, and society bear an immeasurable cost every time an operator collects, uses, or discloses a child's information without parental involvement. Thus, in its cost/benefit analyses, the Commission should compare

---

[33] See, e.g., Disney.com Registration (visited May 11, 1999) <http://disney.go.com/sign-in/>.

[34] Operators will likely benefit financially from any registration process which keeps parental involvement to a minimum. Many Web sites directed at children currently register children automatically with only a brief mention to the child to "get your parent's permission before you sign up." See, e.g., Bonus.com the Supersite for kids (visited May 11, 1999) <http://www.bonus.com>; Purple Moon (visited May 11, 1999) <http://www.purple-moon.com>.

[35] Moreover, because Congress enacted COPPA to protect children's privacy rather than to facilitate data collection, costs to operators should be taken into account only if options are otherwise equal with respect to protecting children's privacy. If operators must bear the costs of information collection from children, they may offer more interactive content to children without collecting information. Such a development would be an additional benefit of requiring non-electronic methods of obtaining verifiable parental consent.

the societal costs of not using verifiable methods of consent with the incremental benefit that operators might receive if they used unverifiable methods, taking into account the fact that operators will receive economic benefits regardless of the consent method employed.

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

Digital signatures would be one such mechanism. In addition, some form of third-party registry may also be possible, but any such system would require privacy safeguards of its own. CME/CFA, et al. are confident that the remarkably innovative online industries will create other cost-effective methods of gaining consent electronically which, unlike e-mail, are truly verifiable.

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

E-mail-based systems of consent have serious costs. E-mail is not a verifiable method of consent because there is no means of ascertaining whether consent granted by e-mail is actually from a parent. Moreover, e-mail-based consent methods encourage an immediate response. CME/CFA, et al. believe that a parent's decision about whether to surrender a child's privacy is one which should be carefully considered rather than rushed. While immediacy may be desirable in some instances, parents should have the option to decide at their own pace whether or not to grant consent. If parents wish to respond immediately, they can do so through a well-managed toll-free telephone-based consent system.

(g) What, if any, other methods of obtaining consent should the Commission consider? Please describe how those methods work, their effectiveness, feasibility, costs and/or benefits, and, if still in development, when they will be available.

Children who access Web sites and online services at schools, libraries, and community centers should be able to obtain verifiable parental consent, even if they do not have computers at

home. Thus, all Web sites and online services should include a toll-free number and/or address so that parents can provide consent through offline means.

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 enables a child to make such information publicly available through, for example, a chat room or bulletin board?

No. Operators can use personal information in a variety of ways that parents may find as objectionable as uses by third parties. In addition, the proposed rule defines the term "operator" broadly to permit the existence of multiple operators for a single Web site. While CME/CFA, et al. support this interpretation, it allows entities to be considered operators regardless of their primary business, as long as they receive information directly from the Web site. Thus, parents may be justifiably concerned about some of the operators' potential uses of children's information.

Chat rooms and bulletin boards may be frequented by individuals who seek to prey on children. Thus, parents must be involved in their children's participation in such activities.

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?

Any system for parental consent will be subject to abuse. In the past, individuals have assisted children in bypassing controls placed upon them by their parents, [36] and instructions for disabling Internet filtering software are freely available on the Internet.[37] Still, while it may be

---

[36] See Jon Katz, "Liberator, Geek Warrior" in The Netizen (April 9, 1997) <http://www.hotwired.com/netizen/97/14/index2a.html> (relating the story of a high school student who disabled filtering software for children).

[37] See "How to disable your blocking software"(visited May 10, 1999) <http://www.peacefire.org/#disable> (explaining how to disable filtering software on a computer surreptitiously).

impossible to completely prevent such counter-efforts, any measure that make parental consent more verifiable will limit them.

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

While additional research may be useful, the Commission cannot wait for such research to be completed before implementing the rule. If future studies demonstrate that some consent mechanisms are more appropriate, the FTC can review them and amend the rules as needed.

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 purposes of this requirement? On what is this estimate of a "reasonable time" based?

The Commission should define "reasonable time" narrowly. The Commission could adopt a three-day waiting period, similar to the "cooling-off period" required for door-to-door sales.[38] Given the nature of the Internet and the attention span of children, parents are unlikely to wait more than a few days to grant or deny consent. However, when adopting a specific time limit, the Commission should consider the method used for obtaining parental consent. For example, parents who provide consent by postal mail should have an extended period of ten business days to respond before an operator deletes their 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?

---

[38] See 16 C.F.R. § 429.1 (providing an individual three business days to cancel a sale made at his home).

While a "do-not-contact" list may benefit some parents who do not wish to be inundated with repeated requests, CME/CFA, et al. believe that such a list might generate more costs than benefits. A "do-not-contact" list limits the flexibility of parents who might decide to grant consent later as their children age or as the Web site changes its policies. In addition, by keeping such a list, the Web site or online service would be preserving parents' contact information, thereby impinging on their privacy. Thus, CME/CFA, et al. recommend that the Commission require that Web sites or online services not automatically include the names of parents who do not consent on a list, but instead, offer parents the option of having their names included. If such lists are offered, operators must provide parents with a simple effective procedure for adding or deleting their name. As an alternative to a "do-not-contact" list, the Commission should also consider limiting the number of times a parent can be contacted by any given operator.

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?

CME/CFA, et al. do not see any need to allow operators to collect more than the child's first name. Parents would need to be informed of the child's name so that they could be sure that they were providing consent for their own child. The collection of any other information from the child would require her to make unnecessary disclosures to the operator.

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?

CME/CFA, et al. find it unlikely that the collection of a child's information could be used to protect that child. CME/CFA, et al. believe that operators should collect a parent's information if they have serious concerns about a child's safety.

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 Web site;
(b) to aid in the judicial process; or
(c) to aid in law enforcement?

This provision could create a loophole for operators to collect and retain information. Thus, the FTC should clearly prohibit operators from construing this provision to permit retention or collection of information that would not otherwise be retained or collected, in anticipation of the possibility of future security or legal concerns.

Indeed, the need for this exception is unclear. Typically, by the time collection of the child's information would become necessary for one of these purposes, the operator would not be able to collect it. For instance, if a child performs an illegal act online, he is unlikely to provide the operator with personal information afterwards. Moreover, an operator is unlikely to have a reason to collect information under this provision unless the child involved is already a participant in interactive activities. In such cases, the operator would already have the name and online contact information for both the parent and the child. In any case, CME/CFA, et al. support the Commission's position that parents should always be notified of information collected under this exception.[39]

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 such

[39] NPRM at 23.

circumstances as the Commission may determine are appropriate, taking into consideration the benefits to the child of access to information and services, and risks to the 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?

To prevent parties from using this "backdoor" to expand the number of exceptions, the Commission should require notice and comment before adopting any new exceptions. Any such exception should be crafted with extreme care.

Right of parent to review personal information provided by child

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?

CME/CFA, et al. support a password-based system for identifying parents, although we recognize that this system is imperfect and may be abused. In a password-based system, a third party could pose as a parent, forge verifiable consent for a child, and then gain access to all of that child's information. Still, relying on a password may be less problematic than requiring parents to submit photocopies of their drivers' licenses. While drivers' licenses may provide better proof of parents' identities, they may also reveal additional personal information to the operator, including the parents' license numbers and social security numbers, which parents should not be required to disclose. Until digital signatures are generally available, CME/CFA, et al. support a password-based system because it is the next best method of verifying parents' identity without the disclosure of sensitive information.

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

23. Section 312.7 prohibits operators 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?

Many Web sites request that children disclose personal information before allowing them to participate on the site. Several Web sites seek information that is not reasonably necessary for the child to participate. For example, Kidscom.com asks children seeking to register on the site to disclose their favorite television show, television commercial, and musical group, as well as their hobbies and career plans.[40] In addition, other Web sites include "optional" requests for information from children.[41] Unfortunately, young children may not be able to distinguish between mandatory and optional questions, and are likely to respond to all requests. Thus, all requests for information that are not reasonably necessary for participating in an online activity should be covered by the rule.

Confidentiality, security and integrity of personal information collected from children

24. Section 312.8 requires operators to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

(b) What practices provide the strongest protection?

---

[40]See "Let's Register" (visited June 7, 1999) <http://www.kidscom.com/orak/registration.html>.

[41]See, e.g., "Join Freezone"(visited June 4, 1999) <http://www.curiocity.com/joinbody_old.html> (asking children if they bought anything online and how many computers there are in their home); "McWorld" (visited June 7, 1999) <http://mcworld.threespot.com/timewarp/capsule/sendstuff.html> **(asking children to name their favorite McDonald's food).**

A variety of practices can be used to increase the safety and confidentiality of data. At a minimum, CME/CFA, et al. recommend the following: that operators use only secure webservers when collecting information from children, that information be placed behind firewalls where it would be appropriate to do so, that information be retained in retrievable form only as long as doing so is necessary, that information is deleted as soon as it is no longer being used, that employees authorized to access data be kept to a minimum, and that only employees who are authorized to access data be permitted to do so.

In addition, operators should be required to provide training for their employees concerning the requirements of the rule. Moreover, operators who offer parents a toll-free telephone number for providing consent must train their employees so that they are able to verify that the caller is the parent of the child from whom the operator wishes to collect information.

Safe Harbor

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?

CME/CFA, et al. support the Commission's position that assessment mechanisms must not be mere self-evaluations.[42] Any independent assessment should be performed by a neutral

[42] NPRM at 29.

entity. To ensure their independence, assessing entities should neither be paid nor chosen by operators or their agents.

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 312.10(b)(3) lists several examples of such incentives. What other incentives exist that would be similarly effective?

The Commission should ensure compliance with safe harbor guidelines by adopting strict incentives. The methods listed in 312.10(b)(3) should not be exclusive of each other. For instance, consumers should always have a right to a redress, including monetary compensation, regardless of what other measures are taken. Also, reports of disciplinary actions must be published in a widely available source and not a limited-circulation trade publication.

Moreover, all operators whose practices violate the guidelines should be referred to the Commission. If an operator does not follow self-regulatory guidelines, it should not be permitted to benefit from safe harbor treatment. In addition to adopting the listed incentives, the FTC should also require that operators who violate guidelines be subject to closer scrutiny, including the investigation of their affiliates and other Web sites.

Conclusion

CME/CFA, et al. urge the Commission to modify its rules in accordance with the comments set forth above. CME/CFA, et al. would welcome the opportunity to participate in a workshop to discuss any of the issues that arise in the implementation of COPPA.

Sincerely,

Katharina Kopp, Ph.D.
Cathy DeLuca
Center for Media Education
2120 L Street, N.W., Suite 200
Washington, DC 20037
(202) 331-7833

Randi M. Albert, Esq.
Jeneba Jalloh, Esq.
Citizens Communications Center Project
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Ave., N.W., Suite 312
Washington, D.C. 20001
(202) 663-9535
Counsel to Center for Media Education, et al.

Mary Ellen Fise, Esq.
Consumer Federation of America
1424 16th Street, NW, Suite 604
Washington, DC 20036

Of Counsel:
Stuart P. Broz
Law Student Intern
Georgetown University Law Center

June 11, 1999

APPENDIX A

Center for Media Education (CME), founded in 1991, is a non-profit advocacy organization that works on behalf of children and families to promote public accessibility and accountability by the media. CME has been working for several years to protect the rights of children online. CME's 1996 report "Web of Deception" prompted the FTC to launch its initial inquiry into the practices of Web sites that target children.

Consumer Federation of America (CFA) is a non-profit association of some 250 pro-consumer groups, with a combined membership of 50 million, that was founded in 1968 to advance the consumer interest through advocacy and education. CFA has worked closely with CME to defend the rights of children's privacy online and jointly published a consumer education brochure for parents and children entitled, "The Internet, Privacy and Your Child – What You Need to Know as a Parent/Keeping Secrets About You on the Internet – A Kid's Guide to Internet Privacy."

The American Academy of Child and Adolescent Psychiatry (AACAP) is a nonprofit professional organization representing over 6,500 child and adolescent psychiatrists. Its members are physicians with at least five years of additional training beyond medical school in general and child and adolescent psychiatry. Its members actively research, diagnose and treat psychiatric disorders affecting children, adolescents, and their families. The AACAP is committed to protecting the well-being and rights of children and their families.

The American Academy of Pediatrics is a non-profit organization of 55,000 pediatricians dedicated to the health, safety and well-being of infants, children, adolescents and young adults. The Academy engages in advocacy and public education, among other things, on the impact of the media on child health and behavior.

Junkbusters Corp. helps consumers defend themselves against intrusive marketing and protect their privacy online. At http://www.junkbusters.com, the company provides extensive free resources for stopping telemarketing calls, unwanted physical mail, junk email, and commercial invasions of privacy on the Internet.

The National Alliance for Non-violent Programming (NANP) is a not-for-profit network of organizations with a long history of effective community involvement and education. Member organizations include the American Medical Women's Association, Jack and Jill of America, Inc., Jewish Women International, the Links, Inc., the National Association of Women Business Owners, National Council of LaRaza, Soroptimist International of the Americas, and YWCA of the U.S.A. With the capacity to reach two million people, NANP builds and supports community initiatives to promote and teach media literacy and non-violence. NANP headquarters in Greensboro, NC serves as the information, technical assistance, materials distribution and network center for member organizations, local initiatives and the general public.

The National Association of Elementary School Principals (NAESP) is dedicated to assuring that all children receive the best education and to the educational excellence and high professional standards among K-8 educators. NAESP serves 28,000 elementary and middle school principals nationwide in Canada and overseas.

National Consumers League (NCL), founded in 1899, is America's pioneer consumer organization. NCL's three-pronged approach of research, education and advocacy has made it an effective representative and source of information for consumers and workers. NCL is a private, nonprofit organization representing the consumer on marketplace and workplace issues.

The National Education Association is America's oldest and largest organization committed to advancing the cause of public education. Founded in 1857, NEA now claims over 2.3 million members who work at every level of education, from pre-school to university graduate programs. NEA has affiliates in every state as well as in over 13.000 local communities across the United States.

Privacy Times, a Washington-based newsletter that covers the information world, is designed for professionals and attorneys who need to follow the legislation, court rulings, and industry developments that frame the ongoing debate about information privacy. Privacy Times covers such issues as the FTC's developing policy for the Internet, credit reports, Caller ID, medical records, "identity theft," the Freedom of Information Act, direct marketing and the European Union's Directive On Data Protection.

Public Advocacy for Kids is a non-profit child advocacy organization devoted to education, health, telecommunication, and parental involvement issues at the federal level. Services provided on a consulting basis include advocacy training, child policy development, organizing for local and federal action, and communications development.