Before the
UNITED STATES FEDERAL TRADE COMMISSION
Washington, D.C. 20580

In the Matter of

Request for Public Comment on the	**)**	**16 C.F.R Part 312**
Federal Trade Commission's	**)**	
Implementation of the Children's	**)**	
Online Privacy Protection Rule	**)**	
Project No. P104503	**)**	

COMMENTS OF THE TOY INDUSTRY ASSOCIATION, INC.

June 30, 2010

In the Matter of

Request for Public Comment on the	**)**	**16 C.F.R Part 312**
Federal Trade Commission's	**)**	
Implementation of the Children's	**)**	
Online Privacy Protection Rule	**)**	
Project No. P104503	**)**	

COMMENTS OF THE TOY INDUSTRY ASSOCIATION, INC.

INTRODUCTION

The Toy Industry Association ("TIA") is pleased to submit these comments in response to the request by the Federal Trade Commission ("FTC" or "Commission") for public comment on its implementation of the Children Online Privacy Protection Act ("COPPA") through the Children's Online Privacy Protection Rule ("COPPA Rule").[1] The FTC has requested comments on the costs and benefits of the COPPA Rule, and whether the COPPA Rule or certain sections should be retained, eliminated, or modified.

BACKGROUND

TIA is recognized by governments and their agencies, non-governmental advocacy groups, consumers, the media and the trade as the authoritative voice of the North American toy industry. Founded in 1916, TIA represents the interests of over 500 member companies that account for more than 85 percent of U.S. domestic toy sales. Members include producers, distributors, and importers of toys and youth entertainment products sold in North America. Associate members include sales representatives, consultants, licensors, toy testing laboratories, design firms, promotion firms and inventors.

TIA members are in the business of creating fun, safe toys for children. As a natural extension of that business, our members are committed to offering entertaining, educational, safe online environments for children. Many of our members host websites that offer games, activities and features for children, and some offer online content for teen and adult collectors. In addition, TIA members may host online stores where parents can shop online.

TIA has long been an advocate of sound and sensible measures to protect children's privacy and safety online. Nothing is more important to our members than the safety of children and the trust of their parents. Therefore, even before COPPA was enacted, our industry supported self-regulatory measures to protect children's privacy through the Children's Advertising Review Unit ("CARU"), measures that are largely reflected in the provisions of COPPA. In addition, TIA has engaged in educational efforts to protect children, including sponsorship of the website www.ToyInfo.org, where parents can find information about CARU and safe, age-appropriate toys for their families. Our comments reflect our members'

[1] 75 Fed. Reg. 17089 (April 5, 2010).

longstanding experience with adhering to COPPA requirements, and address legal, policy, operational and practical aspects of the existing COPPA Rule and implications of possible changes.

COMMENTS

TIA believes that the COPPA Rule has worked well to protect children's online privacy. Changes to the COPPA Rule should not be made lightly; they must offer substantial privacy and safety benefits to both children and their parents without undue burdens on operators. TIA members are therefore deeply concerned that changes to COPPA, in particular redefining what constitutes "personal information," will in fact undermine the goals of COPPA, potentially requiring the collection of more information - including information that many parents would view as "sensitive" - than currently is collected by many websites. Any proposed changes in scope or definitions will require changes to exceptions and other elements of the COPPA Rule.

TIA believes that all the parental consent mechanisms currently recognized in the COPPA Rule remain necessary and valid. Although some might not be frequently used, they are part of the "toolkit" by which operators can obtain verifiable parental consent. Additional flexibility in mechanisms by which parents can be notified or offer consent would be useful, however, consistent with the spirit of the statute.

To the extent that the FTC determines, based on this review, that changes to the COPPA Rule are within its legal authority and merited on policy grounds because of substantial enhancements to children's online privacy and safety, TIA anticipates that the Commission will issue a proposed rule and seek further input on specific rule changes. TIA would provide additional comments at that time.

The FTC has posed a series of important questions, and we provide responses to those questions of most interest to TIA members.

I. GENERAL QUESTIONS

Is there a continuing need for the COPPA Rule as currently promulgated?

TIA members recognize that the success of their businesses depends on the safety of children and the trust of parents. That is why toy industry members supported sensible steps to protect children's privacy even before COPPA was enacted. Under COPPA, website operators may only collect such types and amounts of personal information as necessary to offer a service or activity or perform their obligations. In keeping with this obligation, TIA members often allow children to visit their sites without submitting any information at all, or to anonymously register with a user name and password. TIA members also utilize the exceptions that allow certain types of interactions with children. Where additional personal information is needed to permit participation in a site or activity, parental consent is obtained. In short, as currently promulgated, COPPA helps to provide the level of protection for children that is our industry's highest priority, building on principles established by CARU.

CARU's role in working with advertisers to help improve privacy practices should also be noted; CARU has actively educated companies about COPPA requirements and made recommendations to help them comply through the CARU enforcement process. The record of voluntary compliance with CARU recommendations by the vast majority of companies with whom CARU raises an issue emphasizes the strong and positive role of self-regulation. Other organizations have also developed important self-regulatory programs that help to safeguard the privacy of children.

What impact has the rule had on operators?

The principles set forth in the COPPA Rule were familiar to many of our members active in CARU prior to the enactment of COPPA, and the COPPA Rule has served to create a basic standard for website operators. While the COPPA Rule does impose compliance costs on operators, current definitions of "personal information," exemptions, and options for obtaining verifiable parental consent generally allow TIA members to offer appealing websites to children and to interface with collectors and adult purchasers without undue burden. Nevertheless, two areas in particular merit special attention.

Some TIA members implement age-screening to avoid collecting information from children, coupled with a session or timed cookie to prevent an underage visitor from hitting the back button and registering, even in e-commerce or other areas not intended for children but which children may visit. The single biggest area of consumer complaints that some TIA members have experienced involves adults who enter an incorrect birth date and then are blocked from accessing certain adult-oriented or collector websites or prevented from purchasing products online. While age-screening imposes administrative costs, including time spent in responding to consumers, the larger costs of frustrated consumers simply going elsewhere to make a purchase because they are blocked from a website due to COPPA age-screening cannot be quantified. Consumer frustration, and the burden on operators, will increase even more if the Commission alters the definition of "personal information" in a way that expands the obligation to obtain verifiable parental consent when what is now anonymous information is collected.

Suggestions have been made that websites, in an effort to assure that they are dealing with a parent in obtaining parental consent, collect information that only a parent knows, like the last four digits of a social security number. This will require collecting additional information not currently requested, and cross-checking that additional information against external databases. Requiring parents to share additional information when they already dislike sharing their age - and question why it is being requested - is not likely to increase consumer confidence, but will impose a greater burden on website operators. A more cumbersome age-screening process, coupled with a mandatory verification component, will broadly affect all companies that implement age-screening in an effort to avoid collecting information from children. As a practical matter, a child who obtains a parent's credit card number to access a website could probably also locate and use a parent's social security number, raising questions about whether current recommended methods for obtaining parental consent should be altered to include an added and burdensome verification component.

Does the COPPA rule overlap or conflict with any other federal, state, or local government laws or regulations? How should these overlaps or conflicts be resolved, consistent with the Act's requirements?

Currently there are no legal conflicts between the COPPA Rule and other federal laws, but the potential for conflicts with the rules and regulations of the Federal Communications Commission ("FCC") exists should the FTC determine that COPPA should be extended to other technologies such as interactive television and mobile media. Close inter-agency coordination will be needed in considering application of COPPA to media regulated by another expert agency.

With respect to state and local laws, again there are no existing conflicts. Section 1303(d) of COPPA, 15 U.S.C. § 6502(d), provides that "[n]o State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this title that is inconsistent with the treatment of those activities or actions under this section." Congress concluded that a uniform national standard for the privacy of minors was necessary and desirable, a point with which TIA strongly agrees. Congress recognized that inconsistent state laws that made illegal data collection activities currently legal under COPPA would make it impossible for websites to operate.

II. DEFINITIONS

Do the definitions in 312.2 accomplish COPPA's goal of protecting children's online privacy and safety and are they clear and appropriate?

TIA believes that the current definitions work well. In most cases, the definitions are drawn from the statute itself. For example, the statute defines a "child" to mean an individual under 13. The term "verifiable parental consent" is defined in a flexible way, allowing any reasonable effort, taking into consideration available technology, to ensure that a parent receives notice and authorizes information collection. The Commission has repeatedly recognized e-mail plus as an option for collection of information where internal marketing by the website, with no disclosures to third parties, is involved, because there are reduced privacy risks to children from internal marketing than from disclosures to third parties.

TIA members often offer website content intended for children, as well as websites or content for adults. For sites intended for general audiences, the "actual knowledge" standard is clear. It requires something more than imputed knowledge based on the potential for a child to be interested in the content. Consequently, TIA believes the definitions do accomplish the goal of protecting children's online privacy and safety, consistent with different levels of risk presented by internal marketing versus disclosure to third parties, and the rights of older consumers to obtain information about products and services of interest to them.

Should the definitions of "collects or collection" and "disclosure" be modified to take into account new online technologies or features? How will use of centralized authentication methods such as OpenID affect individual websites' COPPA compliance efforts?

Collection and disclosure restrictions apply to "websites" and "online services" directed to children or those with actual knowledge that they are dealing with a child. Both terms are linked to the definition of "personal information" and to the definition of the "Internet" in the statute. To the extent that new online technologies or features fit the definition of a website or online service, and the website or online service is directed to children or the operator has actual knowledge that it is dealing with a child, such technologies or features may be currently covered by COPPA. Further consideration must be given, however, to applicable legal frameworks under other laws that apply to these technologies. To the extent COPPA is applied to other technologies currently deemed to fall outside COPPA, aspects or limitations of those technologies will likely require revisions to the COPPA Rule. This would include revisions to existing exceptions to allow for appropriate safe interactions with children and to provide a mechanism to offer parental notice and to obtain consent.

As for centralized authentication methods, TIA members have not typically used infomediaries or services such as OpenID. Parents want to interface with brands they know and trust. That is why so many toy company websites are structured to minimize information collection from children. At present, these types of centralized authentication methods do not appear to affect our members' COPPA compliance efforts.

Are there circumstances where an operator using an automated system of review and/or posting meets the deletion exception to the definition of collection and does the Rule provide sufficient guidance on how to handle this?

A variety of automatic filtering techniques exist that are effective and allow companies to take advantage of the deletion exception. The goal is to allow children to enjoy an interactive experience in a safe way. TIA does not believe that the COPPA Rule needs to be amended in this area, or that specific technologies should be mandated. Rather, additional education and information exchanges about techniques that work well may be useful.

What are implications of COPPA enforcement for technologies such as mobile communications, interactive television, interactive gaming, etc., consistent with the Act's definition of "Internet"?

This question requires an analysis of whether all interactive television, mobile communications and interactive gaming platforms constitute websites located on the Internet or online services subject to COPPA enforcement, consistent with the statutory definitions of COPPA, obligations under other laws, and constitutional and public policy considerations. TIA believes that if COPPA is to apply to any of these technologies, clear, common sense standards that allow appropriate interactions with consumers, consistent with the spirit of COPPA and relevant limitations or capabilities of those technologies, are needed.

If one or more of these technologies are subject to COPPA, then the Commission must also consider whether amendments to the COPPA Rule are necessitated by aspects of the specific media involved. For example, the e-mail address of a parent may not be the best way to offer notice or obtain parental consent in connection with mobile media or interactive television use. Amendments would therefore be needed to allow operators to collect a parent's cell phone number or other contact information for purposes of sending a notice or obtaining consent through that technology. Moreover, technical limitations, such as character limitations for text messages, would necessitate altering requirements for the content of parental notices. TIA expects that if the FTC seeks to alter the scope of the COPPA Rule by referencing these technologies, the FTC would issue a proposed rule and solicit public comments on the specifics. TIA would provide further input at that time.

Should the definition of "personal information" be expanded to include other items of information that can be collected from children online, such as persistent IP addresses, mobile geolocation information, or information collected in connection with online behavioral advertising? Do operators, including network advertisers, have the ability to contact "specific individuals"?

TIA opposes expanding the definition of "personal information" to include data elements such as IP address or other information not otherwise included in the current definition, particularly as applied to company websites or affiliated websites. The notice asks whether operators have the ability to contact a "specific individual" using one or more pieces of information, such as user or screen names and/or passwords, zip code, date of birth, gender, persistent IP addresses, mobile geolocation information, information collected in connection with online behavioral advertising, or other emerging information. The types of data defined as "personal" in COPPA are those that would allow an individual child to be physically contacted *directly* by a website operator or online service provider operating a website directed to children or with actual knowledge that they were dealing with a child. The definition of personal information is related to specific exceptions as well, with interactions permitted for appropriate purposes and more robust verifiable parental consent required where there is a heightened safety risk, *e.g.*, where third party or public disclosures increase the potential predator risk. Our comments below address some of these specific data elements and how they might be collected and used separately.

User or screen names, passwords and IP addresses. One of the most important provisions of COPPA is that websites should not collect more personal information than necessary to allow a child to engage in an activity. This is a key guiding principal for toy company websites. Some sites are structured so that children can visit and participate in activities without providing any personal information. Others may collect only a user name and password to personalize the visitor's experience without collecting personal information. A user name and password may relate to a "specific individual," but, unlike an e-mail address of a child used for a one-time contact or an e-mail address of a parent collected to send a notice or obtain consent, this data does not allow that individual to be physically contacted by the website. It simply allows content at the website to be tailored to that user's interests.

All sites automatically log IP addresses of all visitors. At least one court has already found that IP addresses do not constitute personal information. In an order issued last year, the U.S. District Court for the Western District of Washington held that IP addresses are not "personally identifiable information" because an IP address identifies a computer.[2] Only after matching the IP address to a list of an Internet service provider's subscribers can the subscriber be identified. The court clarified that, for an IP address to be personally identifiable, it must identify a *person*.

For over twelve years, websites directed to children have collected anonymous information like a user name and password and automatically logged IP addresses to help personalize a child's experience and to understand traffic at the site. This has always been viewed to be an appropriate way to offer personalization without collection of personal information from children. TIA is unaware of any evidence suggesting a threat to children's privacy or safety that justifies recharacterizing this type of information as "personal." Imagine an Internet universe where a child-directed website would be forced to block visitors until parental consent had been obtained simply because an IP address, user name and password, which do not allow the website or online service to directly contact a child, is recharacterized as personal information. The result will be to require companies to collect even *more* information from a child, such as a child's e-mail address and parent's e-mail address, as soon as a visitor comes to a site, in order to comply with COPPA's parental notice and consent requirements. It is not apparent how this will benefit either children or parents or result in a positive website experience. Expanding the definition in this way, however, will dramatically increase the costs and burdens on website operators.

Age, zip codes, and gender. A child's age, zip code, or gender may be collected on an anonymous basis, without the collection of "personal information," to offer age-appropriate content or obtain general demographic information. That information can be important to toy companies in both updating website content and in product development. A birthdate might be collected with a user name and password to allow a child to join a "birthday club," so that when the child visits the website on her birthday she gets a "personalized" birthday greeting. Of course, to send an e-mail birthday greeting, verifiable parental consent would be needed, and the e-mail plus exception works well for this purpose.

Mobile geolocation information. From TIA's perspective, a careful review of the technology, applicable legal frameworks and existing self-regulatory standards would be needed before proposing to generally categorize mobile geolocation information as "personal information." That does not mean, however, that reasonable and appropriate protections are not desirable, but a combination of the existing requirements of COPPA, laws and rules implemented by the FCC, standards implemented by carriers and industry guidance appear to offer appropriate protection.

Under COPPA, websites or online services directed to children may not collect mobile or home phone numbers from children absent parental consent. Phone numbers, to the extent collected by TIA members, would typically be collected from parents in e-commerce areas or

---

[2] *Johnson v. Microsoft Corp.*, No. C06-0900RAJ (June 23, 2009).

through e-mail plus or other parental verification processes, where clear disclosures about their use would be required. To the extent that TIA members would be interested in using geolocation capabilities to, *e.g.*, send coupons or offers, the intended recipient would typically be the parent. For application providers who allow downloadable geolocation-based applications to be downloaded to devices, the age may not be known.

Mobile phone services are available via subscription and an adult is required to open an account. Like an IP address, the phone number and thus the location of the device may be automatically collected *by the telecommunications service provider* for purposes of providing the telecommunications service. The FCC has authority to regulate telecommunications carriers, and indeed they are pervasively regulated; careful consideration of Communications Act definitions and requirements and the role of carriers is needed before altering definitions and obligations under COPPA. Self-regulation by the carriers is important as well. The Mobile Marketing Association recently updated its *U.S. Consumer Best Practices* (Version 5.1; May 27, 2010), which includes provisions on advertising to children. The mobile marketing community is actively promoting fair and appropriate practices through self-regulation.

Interest-based advertising. Interest-based advertising ("IBA"), sometimes called online behavioral advertising ("OBA"), involves the collection of anonymous information about online activities across the Internet for purposes of serving interest-based advertising. The categories which define those interests are developed by network advertisers. Principal players in IBA are the entities that actually collect the anonymous information and serve the interest-based ads. They are typically members of the Network Advertising Initiative ("NAI"), which has issued and updated its *Self-Regulatory Code of Conduct* so as to achieve an appropriate balance between offering the benefits of targeted advertising while respecting consumer privacy. The NAI principles restrict IBA specifically targeting children without verifiable parental consent. In other words, network advertisers may not create a category of "children under 13" for purposes of serving ads. They could, however, create a category such as "gamer," "movie lover," or the like based on the collection of anonymous information drawn from a variety of websites. The advertising industry has also issued *Self-Regulatory Principles for Online Behavioral Advertising* and is finalizing an enforcement and compliance plan; self-regulation again will offer appropriate protection and has the strong support of major associations representing the advertising industry.

Collection of anonymous information like IP address, operating system, pages viewed, or time spent, helps a website understand its visitors and develop content and offerings of interest based on historic trends. TIA supports the distinction made by the advertising industry in developing recent *Self-Regulatory Principles for Online Behavioral Advertising* between first party site activities and information collected across unaffiliated websites. A first party site includes sites operated by affiliated companies. In contrast, IBA is defined as tracking a visitor across unaffiliated websites using anonymous information for the purpose of offering interest-based advertising. Having closely studied the issue, the entire advertising industry has developed a targeted self-regulatory program applicable to network advertisers or others engaged in IBA across unaffiliated company websites. TIA supports this initiative. Redefining "personal information" in a manner that will prevent existing safe and appropriate practices by toy companies predicated on a common sense understanding of what Congress intended in defining the term "personal information," is not the solution.

Summary. In sum, any decision by the Commission to alter the definition of personal information must be based on some demonstrable privacy harms to children, and then must take into account how changes could affect companies' obligations under other sections of the COPPA Rule and the fundamental functionality of the Internet. To the extent the FTC proposes revisions to the current definition of personal information, TIA would provide further detailed input in response to a notice of proposed rulemaking.

III. NOTICES

Should the notice requirements be clarified or modified to reflect changes in types or uses of information collected from children or changes in communications options available between operators and parents?

Notices to parents largely duplicate information found in the required website notices and obligations of the COPPA Rule itself. TIA believes that this is unnecessary. The key points to communicate to parents are the types of information needed and why, including if, and if so, for what purpose, it may be shared with third parties. If, however, the definition of personal information changes, wholesale review of the notice requirement will be needed. TIA is concerned that notification about collecting information that does not allow a child to be physically contacted directly by the website, such as IP address, will prove confusing to parents.

It was noted at the FTC's June 2, 2010 COPPA Rule Review Roundtables (Roundtables) that adding text message notifications to parents would be a helpful additional option. TIA agrees. Use of the text message format, however, will automatically limit the ability of an operator to include much of the specific information currently found in e-mail notices to parents and will also require revision to allow websites to collect a parent's cell phone number in order to offer notice or obtain consent.

IV. PARENTAL CONSENT

Has the parental consent requirement been effective in protecting children's online privacy and safety? Do the enumerated methods approved by the FTC to obtain verifiable parental consent remain valid? To what extent are methods being used? Should any method be removed or new ones added?

As was noted at the Roundtables, each approved method of obtaining verifiable parental consent is generally effective in protecting children's online privacy and safety. Each has its limitations, but with the exception of digital signatures accompanied by public key technology, all are used by toy companies. The e-mail plus mechanism remains important to the toy industry, and TIA urges that it be retained.

Where effective automated filtering techniques to maintain anonymity in social networking activities are not deployed, more robust methods of verifiable parental consent are required. The most common method used by TIA members to obtain verifiable consent in such instances is to require parents to furnish a credit card number and engage in a transaction. Companies generally have the most confidence in this method, but requiring parents to enter into

a transaction may discourage some parents. Fax back or mailed forms are less common because they must be manually processed, but can be used with the one-time only e-mail approach for certain sweepstakes or contests.

New developments in digital signature technologies or cell phone-based transactions as mechanisms to notify parents and obtain consent merit further analysis as they may offer added flexibility. TIA urges the FTC to explore alternative methods for obtaining consent, such as the use of short codes through mobile phones. Based on discussions at the Roundtables, this method, with today's younger parents who have grown up using cell phones, may prove very effective in reaching a parent. To do so, the COPPA Rule would also have to be modified to allow for the collection of a parent's cell phone number from a child to make that contact with the parent.

V. EXCEPTIONS TO VERIFIABLE PARENTAL CONSENT

Are the exceptions to the prior parental consent requirement being used? Are clarifications or modifications necessary?

The principal exceptions of interest to toy industry members are the one-time only exception and the multiple e-mail exception. The multiple e-mail exception can be the basis for sending news and updates, but more commonly is used in conjunction with sweepstakes or promotions where there may be multiple contacts or with registrations to allow the site to send password reminders. The COPPA FAQs indicate that in order to send e-mail reminders to a child about forgotten passwords, notice to parents is required unless the e-mail address of the child is "hashed" so that the child cannot be contacted but e-mail reminders can be sent, one reason companies may use the multiple e-mail notice exception.

Postal mail notices are not typically used as a parental notification or consent method except in the context of a sweepstakes or contest as part of the prize award process where the initial entry relies on the one-time contact exception.

Other exceptions, like allowing online contact information to be used to protect the safety of a child under Section 312.5(c)(3) of the COPPA Rule, also require reasonable efforts to provide a parent notice and the opportunity to opt-out. There are rare instances where a child might post or attempt to post information that suggests the child is in danger. The website would not have the parents' contact information if it is operating in reliance on certain exceptions. For example, for sites that rely on the deletion exception to offer stripped and screened, white or black list, or other methods to limit postings by children, they may have only a user name and password, and an IP address. In that situation the appropriate course is to contact the IP service provider in an effort to identify the subscriber. A website may also notify law enforcement authorities, implicating the exception under Section 312.5 (c)(4). This again illustrates that IP addresses do not allow direct contacting of the child.

VI. RIGHT OF A PARENT TO REVIEW AND/OR HAVE PERSONAL INFORMATION DELETED

Are parents exercising their rights under Section 312.6(a)?

TIA supports offering convenient mechanisms for parents to request access to information collected from a child. Parents only rarely request access, likely because the principle of limiting collection of personal information from children disclosed in privacy policies and notices helps make parents confident that their children's privacy is protected. Access is generally predicated on a parent filling out and sending a signed, written form that includes a certification statement that the individual signing is the parent of the child in question. Where a credit card in connection with a transaction is used as the parental consent mechanism, the credit card may also serve as a verification method. Parents may also have the ability to review their children's activities and information where sites allow or require parents to set up "family" accounts.

TIA supports the ability of the website operator to choose a verification method that is reasonably calculated to assure that the individual making the request is in fact the parent, consistent with methods currently recognized. Adding an authentication requirement or requiring collection of additional information from parents that children might not know would impose added burdens and costs. There is no indication that the safety and privacy of children has been threatened by use of the approved methods for parental access since COPPA was enacted in a manner that warrants modification.

VII. CONFIDENTIALITY, SECURITY AND INTEGRITY OF PERSONAL INFORMATION

Do operators take seriously the requirement to avoid conditioning a child's participation in an activity on disclosing more information than necessary?

As indicated earlier, limiting collection of personal information from a child to only what is necessary to allow a child to participate in an activity is a core principle for TIA members in operating their websites, consistent with our industry's commitment to safeguarding children and maintaining the trust of parents. That is one reason why the toy industry is concerned about suggestions to expand the definition of personal information. This will create an obligation to collect still more information from children and parents, with commensurate new obligations and costs to manage that data. We believe that such changes will not provide safety benefits to children and are wholly unnecessary, particularly as to company websites and families of websites.

The notice does not refer to the exclusion that allows information to be shared with agents and service providers who help make the website and online offerings available and assist the website operator in business operations. As part of their procedures to maintain the security of children's personal information, website operators typically adopt contractual provisions that restrict the ability of agents and service providers to use information except in connection with

legitimate activities for the website operator. Nevertheless, small businesses may be less aware of the necessity of such provisions in dealing with service providers. The FTC might be able to serve a helpful role in educating small companies and third party service providers about responsibilities with regard to privacy, in particular children's privacy.

VIII. Safe Harbors

Has the safe harbor process been effective? Should it be modified?

TIA has supported the safe harbor component of COPPA, and appreciates the effort that safe harbor organizations and the FTC have made to offer additional guidance and an enforcement mechanism. In that regard, CARU remains active in serving on the front lines of privacy enforcement even with websites that do not participate in its safe harbor, and the availability of multiple safe harbor programs offer choices to those who wish to avail themselves of those services. The current criteria used to evaluate safe harbor applications appear to be working successfully. TIA does not believe that a formal periodic reassessment program would be necessary or useful. At the same time, we believe that should the Commission become aware that a safe harbor participant is not adhering to the commitments that formed the basis of the approval, it has ample authority to revoke the status.

IX. Statutory Requirements

Does the commenter propose modifications that conflict with the statute or propose seeking legislative changes?

TIA's suggestions for added flexibility by relying on expanded notices and new mechanisms for parental consent do not require statutory changes. We believe that altering the definition of personal information to include user name, password and IP address- data elements that do not allow a child to be directly contacted online or offline- is contrary to the letter and spirit of COPPA. Such a change is unmerited based on privacy harms to children. COPPA has generally worked well. As such, changes that would negatively affect user experiences and prevent toy companies from continuing to offer entertaining features for children and information and products for adults should be avoided.

CONCLUSION

As a strong advocate for children, TIA appreciates the opportunity to submit comments to the FTC in this important proceeding. The COPPA Rule has been effective in protecting children. Any changes to the COPPA Rule must be thoroughly examined to be sure they are consistent with the statute, reflect sound public policy, are technologically appropriate, and can be implemented in a common sense manner. The costs and benefits of any changes must be weighed to avoid any unnecessary and unintended adverse effects on both consumers and on companies that must comply.

Respectfully Submitted,

Carter Keithley
President
Toy Industry Association, Inc.

Of Counsel:
Sheila A. Millar
Tracy P. Marshall
Keller and Heckman LLP
1001 G St. N.W., Suite 500 West
Washington, D.C. 20001