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	**)**	
Proposed Revisions to the	**)**	
Children's Online Privacy	**)**	
Protection Rule, Project No. P104503	**)**	

COMMENTS OF THE TOY INDUSTRY ASSOCIATION

September 24, 2012

In the Matter of

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

COMMENTS OF THE TOY INDUSTRY ASSOCIATION

INTRODUCTION

The Toy Industry Association ("TIA") is pleased to submit these comments in response to the Federal Trade Commission's ("FTC" or "Commission") Supplemental Notice of Proposed Rulemaking and request for further public comment on its proposed revisions to the Children's Online Privacy Protection Rule ("COPPA Rule" or "Rule"), promulgated under authority of the Children's Online Privacy Protection Act ("COPPA").[1] On September 27, 2011, the FTC issued a Notice of Proposed Rulemaking ("2011 NOPR") setting forth proposed changes to the COPPA Rule[2] on which TIA previously submitted comments, which are attached hereto and incorporated herein by reference. The FTC is now proposing to further modify the proposed definitions of *personal information*, *support for internal operations*, and *website or online service directed to children*, and further proposes to revise the Rule's definition of *operator*. TIA's members have a strong commitment to privacy in general, and to children's privacy in particular. The proposed, further revisions to the Rule include some useful modifications that may help facilitate our members' ability to offer fun, safe online environments for children. However, the Commission's proposed revisions and further modifications continue to raise concerns within the toy industry.

BACKGROUND

TIA is recognized by governments, 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 550 member companies that account for more than 85 percent of the U.S. domestic toy market. 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.

Safeguarding children and earning the trust of parents continues to be a central part of our members' businesses. These principles are at the core of our industry's commitment to privacy. Toy companies have not only created fun, safe toys for children, but have also offered

[1] 77 Fed. Reg. 46,643 (August 6, 2012) ("Supplemental Notice").

[2] 76 Fed. Reg. 59,804 (September 27, 2011).

entertaining, educational, and safe online environments for kids. Our industry remains committed to ensuring that sensible children's privacy rules reflect changing technology, as well as practical business realities that reflect these core principles. However, toy companies also view parents and teens to be an important audience. Many TIA members host websites that offer online content for teen and adult collectors, online stores where parents can shop, and apps for general audiences or families. Thus, ensuring the privacy of consumers of all ages is very important to TIA member companies.

TIA appreciates the opportunity to provide further comments on the FTC's proposed revisions to the COPPA Rule. These comments reflect our members' longstanding experience with adhering to COPPA requirements, and address legal, policy, operational, and practical aspects of the existing COPPA Rule and implications of possible revisions. We look forward to working with the Commission as it moves forward with its revisions to the COPPA Rule.

EXECUTIVE SUMMARY

TIA appreciates the Commission's thoughtful consideration of many of its comments to the 2011 NOPR. The Commission has taken some very important strides in issuing the Supplemental Notice. However, the changes do not go far enough and may adversely affect current activities that clearly fall outside the scope of COPPA. Some of the revisions proposed by the FTC are not necessitated by evidence of privacy or security risks to children, but will exponentially increase the burdens of COPPA compliance for website operators, service providers, children, and parents alike. Specifically:

- The revised definition of an *operator* in the Supplemental Notice will present significant administrative and operational concerns. In conjunction with the earlier proposal that the name and address of all operators appear in privacy notices posted online, the expansive definition will further complicate the process of drafting and updating online privacy notices, making them more complex and confusing to consumers, and potentially necessitating more frequent updates as business relationships change. Further, TIA members are deeply concerned that the proposed change may cause a number of business partners to either severely limit or even discontinue commercial relationships with toy companies, since support for child-directed websites and services may simply be a very small portion of revenues. Alternatively, they may impose untenable or unaffordable fees on toy companies to shift the costs associated with complying with the COPPA Rule. The FTC should continue to require that operators exhibit some sort of independent retention of ownership, control, or access to the personal information collected at the website or online service to be considered a "covered operator," rather than including those that collect in the interest of, as a representative of, or for the benefit of another operator. These entities, which include advertising agencies who may manage URLs or data on behalf of a client, web hosting and storage companies, or cloud-computing companies, have historically been considered *agents* of the operator.

- In response to recommendations that it consider ways to address "family oriented" websites, the Commission has offered new language for the definition of a *website or online service directed to children* to allow age-screening. TIA members believe that

offering more options to promote family-friendly content, without requiring that the entire site or service be deemed as directed to children, is a good start. As proposed, however, the Commission's definitions seem to eviscerate the statutory actual knowledge standard and could impose new burdens on toy company sites directed primarily to adults. While the NOPR clearly and properly rejected demographic traffic standards or a "reasonable knowledge" standard to identify sites directed to children, the revisions appear to embrace these previously-rejected concepts. The result could be much broader age-screening obligations on sites that are simply not directed to children. Coupled with fewer, and more complicated options for obtaining verifiable parental consent given the NOPR's proposal to remove e-mail plus, this could increase burdens absent further clarification that certain sites, such as e-commerce sites, are not child-directed.

- TIA appreciates the FTC's revisions to instances where a *screen or user name* is not deemed covered *personal information*, but believes that the proposed revisions do not go far enough. Screen and user names should never be considered *per se* personal information. Anonymous services that allow children to communicate with each other using screen or user names, such as in-game chatting or showcase leaderboards, should be allowed, so long as competent filtering technologies are used to prohibit the disclosure of other personal information. The FTC's revised definition would put such activity at risk, to the extent that posting a screen or user name is viewed as "online contact information," even though outside the gaming or site universe visitors have no ability to contact one another. Further, website operators should be allowed to retrieve and send forgotten passwords when requested. Under the FTC's proposed revisions to a *screen or user name*, these types of activities could be covered as "personal information," even though no personal information is actually being collected from the child.

- TIA appreciates the Commission's proposal to broaden the definition of activities that *support the internal operations of a website* and limit instances when device and persistent identifiers will be considered *personal information*. While helpful, the changes do not cover the suite of activities that we think should be excluded from required notifications and verifiable parental consent through this definition, and we recommend further revisions to cover those activities. As discussed above, agents and service providers should not be considered "operators."

- The Commission acknowledges that the proposed changes outlined in the Supplemental Notice will result in more websites and online services being subject to the Rule, and solicits additional input on the impact. TIA concurs that compliance obligations will be greatly expanded. The staff, however, did not adequately assess input offered by TIA on the costs of the earlier proposal. The Commission must fully evaluate all input to accurately develop the best available cost/burden estimates in accordance with applicable requirements.

- The Commission is not proposing to alter some aspects of the proposed Rule criticized by TIA and others in comments to the 2011 NOPR. For example, a photograph, video, or audio file containing a child's image or voice is *per se* personal

information based on the prior proposal. This does not make sense, particularly since the Commission earlier embraced broader use of reasonable filtering techniques to restrict public posting or display of personal contact details. E-mail plus will continue to be barred under the revised proposed rule despite any indication that its use has not proven harmful to children's privacy. Provisions requiring that operators "ensure" that agents comply with COPPA have not been changed. The Commission must also confirm that "send a friend" e-mails remain permitted in accordance with Commission Guidance. These, coupled with other changes in the Supplemental Notice, will present serious and costly practical, technical, and operational challenges to operators if the FTC fails to revise them.

COMMENTS

TIA continues to believe that the COPPA Rule has worked well to protect children's online privacy. We appreciate some of the changes the FTC has suggested to minimize some impacts of the revisions proposed in the NOPR and Supplemental Notice, but the changes do not fully address previously stated concerns. The net result of the combination of changes the FTC has proposed in the NOPR and Supplemental Notice creates serious concerns for TIA members. TIA members are troubled that elements of the Supplemental Notice will further undermine the goals of COPPA and will continue to impose significantly greater burdens on operators and service providers, potentially resulting in less content and offerings for children as a result. We provide below our comments on the issues of most importance to TIA members and attach and incorporate by reference our prior comments to the 2011 NOPR.

I. DEFINITION OF *OPERATOR*

In the 2011 NOPR, the FTC did not propose to change the definition of *operator*. Instead, the Commission said it interpreted the term to cover operators of mobile and other online services, such as Internet-enabled gaming platforms, voice-over Internet Protocol ("VOIP") services, geolocation services, premium testing, and coupon texting programs. The Supplemental Notice now proposes to modify the definition of an *operator* to establish that information is "*collected or maintained on behalf of*" an operator when it is "collected in the interest of, as a representative of, or for the benefit of, the operator."[3] This proposed revision directly undermines activities that support the internal operations of the website or online service.

Since the Commission first adopted the COPPA Rule, it has consistently interpreted the "on behalf of" language to exclude instances where the website merely acts as the conduit through which the personal information flows to another, and the website or online service does not have access to the information. To be an *operator* typically required some sort of retention of ownership, control, or access to the personal information collected. ISPs, technology service providers, advertising agencies, and similar entities were never thought to be covered by COPPA. Again, TIA stresses that the underlying principles of COPPA were predicated on collection of the type of information that allowed a child to be directly contacted, online or offline, by the website or online service. The structure of COPPA's parental notice and consent

[3] 77 Fed. Reg. at 46,644.

requirements clearly establish that the most overriding concern was the potential for children to be exposed to child predators. The existing rule has always recognized the common sense reality that many service providers and agents help maintain a website or online service, and these entities have never been considered "operators."

Given changes in technology, the Commission now says it believes that "an operator of a child-directed site or service that chooses to integrate into its site or service other services that collect personal information from its visitors should be considered a covered operator under the Rule."[4] The "operator" of the child-directed site is, of course, already subject to COPPA; the change is intended to expand the reach of COPPA to include linked sites, implicating not only social networking or other types of "plug-ins," but also third party sites. The FTC asserts that these entities are in the best position to know that its site or service is directed to children and can control which plug-ins, software downloads, or advertising networks it integrates into its site. However, the Commission cannot square this with the general statement that links alone do not make another site child-directed,[5] and this new rule will be unworkable in practice.

The Commission explains that the plug-in scenario "mirrors" the current situation with child-directed websites and advertising networks, *i.e.*, the site determines the child-directed nature of the content, but the third party advertising network collects persistent identifiers for tracking purposes. These changes, however, present several administrative and operational concerns for the primary operator of a website or service directed to children, including, in particular, implications to: (1) online privacy notices; (2) direct notices to parents; (3) commercial relationships with providers of software, plug-ins, and others, as well as social media activities; (4) user experience on websites directed at a general audience; and (5) new obligations that operators "ensure" the confidentiality, security, and integrity of personal information.

A. FTC Has Not Addressed the Implications of the Expanded Definition of an "Operator" with Obligations to Identify Them All in Online Privacy Notices

In the 2011 NOPR, the FTC proposed that operators provide contact information for *all* operators of a website in the online privacy notice, rather than designating a single operator as the contact point.[6] Because the FTC has not proposed to revise this requirement in the Supplemental Notice, this would effectively require privacy notices to include contact information for all entities currently deemed agents or service providers who allow links to social networks, downloadable software kits, or other plug-ins to be posted to, or used on, an operator's website.

Furthermore, the Commission's proposed revisions to the definition of *operator* are in direct conflict with its proposal in the 2011 NOPR to streamline the content of the notice of information practices that an operator must provide in its privacy policy. Specifically, the NOPR proposed to eliminate the Rule's "current lengthy" recitation of an operator's information collection, use, and disclosure practices in favor of the following information: "(1) what

[4] *Id*.

[5] 16 C.F.R. § 312.2; *see also* 77 Fed. Reg. at 46,653.

[6] 76 Fed. Reg. at 59,815.

information the operator collects from children, including whether the website or online service enables a child to make personal information publicly available, (2) how the operator uses such information, and (3) the operator's disclosure practices for such information."[7] However, if website operators are required to list all "operators" covered under the proposed definition, and then list the information collected by each operator, how each operator uses such information, and each operator's disclosure practices, consumers are likely to be presented with too much information. Moreover, absent lengthier online privacy notices, consumers may actually be unable to determine from this information who actually provides what services, what those services actually do, and which "operator" the consumer should contact with questions or concerns about such service. The challenge will be magnified in the app space.

This, combined with the overly expansive definition of "personal information" and still unduly narrow definition of "support for the internal operations," effectively may require companies offering websites or online services to children to update their online privacy policies on several occasions each year to reflect work with different entities that may now be considered "operators" whose contact details and practices must be listed in the principal operator's posted privacy notice.

The FTC has failed to respond to or address these concerns in its Supplemental Notice. TIA assumes that the addition or elimination of an "operator" constitutes a "material change," requiring individual notice to and consent from parents. Of course, operators who maintain child-oriented websites, but seek to maintain an anonymous experience for children, may not, as a practical matter, be in a position to provide direct parental notices. The net result could be to force companies to collect more information from children and parents, and to obtain verifiable parental consent, to allow a child to interact, anonymously, with a site, in the same manner they do today, simply as a result of arbitrary new definitions. This is hardly in the best interests of either children or parents.

This change, if implemented, will impose significant new costs and burdens on companies offering child-directed online services or websites that were not taken into account by the FTC. Specifically, if it is the website owner's responsibility to include detailed information on the data collection practices of an expanded universe of entities that are now "operators," then the website owner will incur additional administrative and financial costs, updated online privacy notices will be more frequent, and in order to provide direct notices to parents, websites directed to children may have to entirely restructure operations to obtain parental consent at the start.

B. Commercial Relationships May be Burdened by the Proposed Revisions

The proposed revisions to the definition of *operator* could also pose problems to website operators when it comes to their commercial relationships with others. While the FTC's Supplemental Notice acknowledges that a strict liability standard is unworkable for advertising networks or plug-ins because of logistical difficulties such services face in controlling or monitoring which sites incorporate their online services, redefining a website or online service directed to children to include a commercial website that knows or has reason to know it is collecting personal information from a covered website will have enormous practical

[7] *Id*.

implications and affect contractual and licensing arrangements. While the FTC has stressed that this "reason to know" standard "does not impose a duty to ascertain unknown facts, but does require a person to draw a reasonable inference from information he does have," a modified rule will translate into potential limits on the ability of a child-directed website to use third party technology, and increased costs.

Some advertisers and other partners, especially those in the social media context, may choose to limit services to toy companies if they are deemed "covered operators" under the COPPA Rule. Still, some business partners may choose to prohibit use of their technology on child-directed websites altogether, implicating both content and functionality. In this regard, the implications of new definitions of a *website directed to children* also create concern. For example, on child-directed sites that use web-based technology, like Adobe® Flash, to provide in-browser games or other animations, Adobe may be considered an "operator" under the proposed definition should it collect IP addresses or other information for licensing and updating purposes. The type of information these entities collect has been deemed anonymous since COPPA was first enacted. These entities may take the position that they will no longer offer or permit use of their technology at child-directed sites due to potential risks associated with a newly-expanded COPPA obligation, since a commercial agreement with a child-directed website could meet the "knows or has reason to know" standard. Alternatively, business and advertising partners may choose to impose untenable or unaffordable fees in order to shift costs associated with complying with the COPPA Rule to owners of sites that the owner does intend to direct to children. This may make it uneconomic for sites to continue to offer child-oriented content.

By potentially discouraging "best in class" software providers, or advertising enablers, from working with sites directed to children, innovation within the children's advertising universe may be stifled. Access to audiences may be severely limited as a result, and there is little question that when this occurs, children will seek other sites that offer a richer interactive experience.

C. Impaired User Experience on Websites Directed at a General Audience

Should advertisers and other partners choose to limit or prohibit services, as discussed above, these restrictions may adversely affect not only websites directed to children, but also websites directed to a general audience and operated by the same owner. In this regard, TIA disagrees strongly with the revised definition of a website directed to children under 13. Implications of a "likely to attract children" coupled with a "disproportionately large" standard has implications for e-commerce sites, for example. Given the FTC's proposed revisions to the definition of a *website or online service directed to children*, the proposed changes, and resulting consequences, could alter the default adult experience on sites such as toy company e-commerce sites featuring their toys.

There is no reason that sites which cater to a general audience should now have to treat all users as under 13 by instituting age-screening, especially if the under-13 traffic is merely a minority of the actual traffic. Age-screening, verifiable parental consent, and other procedures simply did not apply to e-commerce sites before these revisions, and should not apply to them now.

D. Procedures to Protect the Confidentiality, Security, and Integrity of Personal Information are Complicated by These Proposed Revisions

The 2011 NOPR proposed to amend the COPPA Rule to add the requirement that "operators take reasonable measures to *ensure* that any service provider or third party to whom they release children's personal information has in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information."[8] The Supplemental Notice would further expand and complicate operators' obligations in this area.

As TIA discussed in its comments to the 2011 NOPR, it is not clear what the FTC means by the word "ensure." Operators regularly investigate agents, service providers, and business partners to assure that they will responsibly maintain the security and confidentiality of children's data, and require contractual assurances of compliance, but are not guarantors of third party actions. The proposed revisions, however, imply that operators have to audit every advertising agency, every social networking site, every software or app used, every third party "plug-in," every advertising or business partner, or any other third party, whose technology is integrated into the operator's site or service that collects information from its visitors.

Requiring companies to go beyond reasonable due diligence, by effectively mandating audits of all third party processes or activities, would impose an undue burden on operators of child-directed sites. Furthermore, the FTC has not articulated what the standard should be for such audits, whether it should be a "reasonable measures" standard, industry standard, or something else. TIA objects to a requirement that operators "ensure" compliance with COPPA. This goes beyond what can reasonably be expected. TIA reiterates that the Commission should clarify what procedures operators would need to have in place to "ensure" that a service provider or third party has reasonable measures in place.

At the very least, the Commission must take into account that such expanded obligations will impose significant added costs on child-directed website operators. These costs will be in the form of additional personnel, tracking tools, and other methods required to police compliance with the expanded definition. Companies would need to devote staff, time, and other resources to enforcement, which could dramatically impact the business costs for a given franchise or product line. As indicated later on in these comments, large multi-URL operators may have to devote 20 hours a week to oversight and compliance with expanded COPPA compliance obligations. Additional risk and costs include the potential delay to enter the market with a new campaign, product, or service, which might result in lost sales or decreased competitive advantage. Operators of websites directed to children are not and cannot be guarantors of the practices of other third parties.

II. DEFINITION OF WEBSITE OR ONLINE SERVICE DIRECTED TO CHILDREN

In the 2011 NOPR, the Commission proposed minor revisions to the definition of a *website or online service directed to children* to include additional indicia of child-directed sites or services. The Commission has always recognized that a website or online service directed to

[8] *Id*. at 59,821 (emphasis added).

children must actually be *targeted* to children to fall within the requirements of COPPA and the COPPA Rule. With this Supplemental Notice, the FTC is proposing to further revise the definition of a *website or online service directed to children* to go beyond those websites that actually target kids. Specifically, the definition of a *website or online service directed to children* would be revised to include a site or service that:

(a) *knowingly targets* children under 13 as its primary audience; or

(b) is based on the overall content of the website or online service, *is likely to attract* children under age 13 as its primary audience; or

(c) is based on the overall content of the website or online service, is likely to attract an audience that *includes a disproportionately large percentage of children* under 13 as compared to the percentage of children in the general population unless it does not collect personal information prior to collecting age information and prevents the collection, use, or disclosure of personal information from visitors identified as under 13 absent verifiable parental consent; or

(d) *knows or has reason to know* that it is collecting personal information through any website or online service covered under paragraphs a-c.[9]

These revisions, quite simply, contravene the statutory "actual knowledge" standard and disregard the Commission's earlier rejection of a "reasonable efforts" or "constructive knowledge" standard in the 2011 NOPR. The two standards are also internally inconsistent. The reference to the "primary audience" in (b) appears to conflict with the "disproportionately large percentage" language in (c), creating significant confusion about what standard applies and under what circumstances. The notion of establishing a demographic standard to identify a "child-directed" site was specifically rejected by the FTC in its 2011 NOPR. Apart from the statutory barrier that bars the FTC from undermining the actual knowledge standard, the change will result in much broader age-screening obligations, with attendant costs.

A. Implications to COPPA's "Actual Knowledge" Standard

Currently, COPPA and the COPPA Rule define a *website or online service directed to children* to include some general indicia. It also covers websites or online services with actual knowledge that they are dealing with a child. The Rule applies to an "operator of a website or online service directed to children, or any operator that has *actual knowledge* that it is collecting or maintaining personal information from a child."[10] This requirement is not being amended under the proposed revisions to the COPPA Rule, and would continue to be in place. However, the proposed revisions effectively change the statutory actual knowledge standard by including demographic benchmarks or a "knows or has reason to know" standard.

The Commission explains that these revisions are being made in order to make clear that a website or online service that knows or has reason to know that it collects personal information from children through a child-directed website or online service is itself directed to kids. This is a tautological argument. These revisions would significantly modify the existing definition that

[9] 77 Fed. Reg. at 46,646 (emphasis added).

[10] 16 C.F.R. § 312.3; 15 U.S.C. § 6502(a)(1).

looked at the intent of the website owner in targeting children as a primary factor in identifying child-directed websites.

Establishing a "knows or has reason to know" standard contravenes the statutory "actual knowledge" standard, which is applicable to sites that are not "child-directed." Actual knowledge is generally understood from case law to establish a far stricter standard than constructive knowledge or knowledge implied from the ambient facts.[11] In fact, the Commission recognized in the 2011 NOPR that actual knowledge is far more workable, and provides greater certainty, than other legal standards that might be applied to the universe of general audience websites and online services.[12] As the Commission has acknowledged, imposing a lesser "reasonable efforts" or "constructive knowledge" standard might require operators to "ferret through a host of circumstantial information to determine who may or may not be a child."[13]

Further, the Commission's proposed revisions to the definition of a *website or online service directed to children*, would not be entitled to deference under the principles set out in *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.* and its progeny. Under *Chevron,* courts will defer to an agency's interpretations of a statute the agency administers only when Congress has not spoken to the precise issue in question.[14] An agency's interpretation will not be entitled to *Chevron* deference when the statute is clear on its face. In this instance, Congress has erected a clear standard that sites or services which are not "directed to children" must have *actual knowledge* that they are collecting information from a child before being subject to the requirements of COPPA and the COPPA Rule. The FTC cannot contravene Congress' intent by establishing a "knows or has reason to know" standard.

As discussed in our comments to the NOPR, the retention of the actual knowledge standard is very important to TIA members who offer sites or areas, like e-commerce sites, that primarily target adults. This effective change to the actual knowledge standard not only violates Congressional mandates, but in practice would force unduly burdensome operational and technical revisions to most toy company websites. In effect, the revisions would create a situation where a user may need to engage in an age verification process each time the user accesses a website designed for a broader audience that might "appeal" to children, or even a website that is located within a "family" of websites owned by the operator because there is a chance that the FTC, under its unclear "disproportionately large" standard, would determine that this type of historically general-interest site is "child-directed." This should not be the default experience for adults visiting general audience or adult-targeted sites, which also happen to have under-13 traffic.

The toy industry, in general, has a very sizable adult collector and adult consumer base. The collection of data at e-commerce sites is presumed to relate to an individual over the age of 13, and there is no basis to impose an imputed knowledge standard upon these websites. Simply

---

[11] 76 Fed. Reg. 59,806 (citing *United States v. DiSanto*, 86 F.3d 1238, 1257 (1st Cir. 1996) (citing *United States v. Spinney*, 65 F.3d 231, 236 (1st Cir. 1995))).

[12] *Id*. at 59,806.

[13] *Id*.

[14] *Chevron USA Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837, 842-843 (1984).

because a website or mobile app features a beloved toy character, including in an area geared to adult collectors or purchasers at online stores, should not automatically mean that it is targeted to children.

TIA urges the Commission to disavow the proposed changes and to retain the *actual knowledge* standard, as is required under COPPA. Should the FTC revise the definition of a *website or online service directed to children*, it must provide some leeway so that "knowledge" of whether the site or service is targeting children, adults, or both, is reviewed and subsequently applied on a case by case, or campaign by campaign, basis.

B. Broader Age-Screening Requirements

In response to a comment received on the NOPR, the Commission has proposed to establish broader age-screening requirements for operators of family-oriented sites. Specifically, the Commission proposes that "sites and services with child-oriented content appealing to a mixed audience, where children under 13 are likely to be an over-represented group, will not be deemed directed to children if, prior to collecting any personal information, they age screen *all* users."[15]

The Commission explains that these revisions are intended to permit a website or online service that is designed for both children and a broader audience to comply with the COPPA Rule by using age-screening mechanisms. As a result, they could be helpful to toy companies that offer family-oriented content, allowing certain information collection to occur where an individual visitor is identified, through age-screening, to be over 13. This proposed revision, however, could effectively result in much broader age-screening obligations that implicate sites and areas, like adult collector and e-commerce sites, that are not targeted or directed to children.

One might, for example, suggest that an online store that offers toys is "appealing" to children. The implication of the revised rule, however, is that a toy company operating an online store that may be linked to other sites directed to children must conduct age-screening at all URLs on this basis. Would this same requirement apply to Amazon, eBay, and other e-tailers that sell toys? Would obligations apply only to third-party e-tailers that offer a specific toy store or area? These are important questions that must be clarified to avoid overbroad application of any new rule. Notably, some toy companies do institute age-screening for newsletters and other features. Some report that existing age-screening practices generate significant complaints from adults who question the reason behind the request for their birth date. While TIA supports appropriate neutral age-screening, application of this change requires significant additional explanation to assure that it is not applied in an overly broad manner, and confirmation that the Commission does not intend for this new rule to apply to online stores, collector sites, corporate sites, or third party advertiser sites that may be accessible to child visitors via links from a child-oriented site.

[15] 77 Fed. Reg. at 46,646.

C. Establishing a Demographic Standard

The Commission has also proposed to include websites or online services that are "*likely to attract children under age 13 as its primary audience*" or "likely to attract an audience that *includes a disproportionately large percentage of children under 13* as compared to the percentage of children in the general population."[16] This would effectively allow the FTC to apply (without expressly establishing) a demographic traffic standard to identify a "child-directed" site, although that concept was specifically rejected in the NOPR. In the 2011 NOPR, the Commission made clear that its past experience with online audience demographic data, in both its studies of food marketing to children and marketing violent entertainment to children, demonstrated that such data is neither available for all websites and online services, nor is it sufficiently reliable.[17] Thus, it declined to adopt a *per se* legal standard.

TIA finds it difficult to square these two separate demographic concepts of the "primary audience" or "disproportionately large percentage" of children under 13. With an increasing number of children online, the FTC has not indicated how it proposes to establish either benchmark. If the FTC decides to maintain this standard in the final Rule, it should explain what threshold it will use to determine a "primary audience" and "disproportionately large percentage." With the growing number of children interfacing with computers and mobile devices, and using the Internet or apps, previous assumptions about levels that are "disproportionate" are likely to quickly change.

III. DEFINITION OF PERSONAL INFORMATION

The types of information that are currently defined under COPPA and the COPPA Rule as "personal" are those that would allow an individual child to be physically contacted directly by a website operator or online service provider that either operates a website directed to children, or has actual knowledge that it is dealing with a child. In the 2011 NOPR, the Commission proposed to redefine the term "personal information" to include data it previously deemed anonymous, including screen or user names, persistent identifiers, geolocation information, photographs, video and audio files, and any information combined with an item of personal information, as personal information.[18]

TIA is pleased that the FTC has taken some of its comments on the 2011 NOPR into account and has proposed to revise the definition of "personal information" by making modifications to *screen or user names* and *persistent identifiers*. TIA believes that these are important changes by the Commission to allow toy companies to continue to provide fun activities in a way that protects children's personal information online. TIA, however, still has serious concerns with the revised definition of a *screen or user name*, and the proposal to include *persistent identifiers*, particularly in light of the expanded definition of an *operator*. In addition, the Supplemental Notice fails to address concerns TIA identified with the inclusion of photographs, videos, and audio files containing a child's image or voice, as personal information.

---

[16] *Id*.

[17] 76 Fed. Reg. at 59,814.

[18] 76 Fed. Reg. at 59,810-59,813.

Pictures, videos, and audio files, without more, do not allow a child to be contacted online or offline.

A. Screen or User Names

TIA appreciates the FTC's revisions to the definition of a *screen or user name.* While these revisions are a good first step, they do not address all the concerns TIA expressed in its earlier comments to the 2011 NOPR. Providing children with the ability to enjoy online activities anonymously by registering with a user or screen name is central to many TIA members' kid-directed websites and online activities. Many toy company sites are structured to collect only a user name and password to personalize the visitor's experience or recall a user's favorite area of the site without collecting personal information. Thus, TIA suggested that a screen or user name should not be included in the definition of "personal information" if it does not reveal an individual's e-mail address or identity.

The Supplemental Notice proposes to modify this definition so that it is considered "personal information" only when it functions in the same manner as *online contact information*. In such a case, the screen or user name would have to function much like an e-mail address, an instant messaging identifier, or any other similar identifier that would permit a child to be directly contacted, in order to be considered personal information. TIA appreciates the FTC's considerations of comments in this area, but believes that the FTC's proposed revisions do not resolve concerns about allowing children to enjoy an interactive experience in an anonymous way.

On many child-directed websites, screen or user names are used to allow children to communicate anonymously with each other (for example, through in-game chatting using filters like white lists, black lists, algorithmic systems, or pre-selected dialogue) or are used to showcase leaderboards for website games. Screen or user names are also used to allow website operators to retrieve forgotten passwords. These types of activities, while allowing a child to be "identified," do not reveal the child's identity or any personal information of the child. They are essential to providing online activities anonymously on kid-directed sites. Indeed, the FTC has recognized that competent filtering technologies may be used to prevent a child's public disclosure of his or her information.[19] Thus, the Commission should not include a screen or user name in the definition of *personal information* if the screen or user name does not reveal an individual's e-mail address or identity, or if the operator uses competent filtering technologies to prohibit the disclosure of other personal information that would allow the child to be contacted online or offline.

B. Persistent Identifiers

TIA appreciates the Commission's proposed revisions to *persistent identifiers* to address a number of concerns that were raised by TIA and other industries. Specifically, the Supplemental Notice intends to address concerns raised about the lack of clarity with including both "persistent identifiers" and "an identifier that links the activities of a child across different Web sites or online services." The Commission's proposal would combine the two previous

[19] *Id*. at 59,826.

definitions into one, and makes clear that a *persistent identifier* is included in the definition of *personal information* only when it can be "used to recognize a user over time, or across different Web sites or online services," and when "used for functions other than or in addition to support for the operations of a website or online service."[20]

The Supplemental Notice does narrow the scope of the impact on operators, and the Commission acknowledges concern that the definitions, as initially proposed, would significantly implicate authentication, site navigation, user preference, contextual ads, site performance assessment, and analytics. However, further clarifications to this definition would be helpful. For example, the definition should be revised so that *persistent identifiers* must be "used to recognize a user over time" and (not "or") "across different Web sites or online services." This revision would ensure that site performance assessments and preferences at a site (or family of sites) does not run afoul of the revised Rule, and that third parties who provide analytical support are not *operators.*

Regardless of the Commission's revisions in this area, *persistent identifiers* are still otherwise *per se* "personal information" even when they may not be linked to another item of personally identifiable information. TIA incorporates by reference the concerns it expressed in the comments to the 2011 NOPR: the collection of one or more persistent identifiers, such as a customer number held in a cookie, IP address, processor or device serial number, or unique device identifier (UDID), only permits contact with a device and not with a specific individual. Legally, the expansion of persistent identifiers as *per se* personal information is out of sync with industry norms and case law, and places an undue burden on U.S. companies to comply with an overly restrictive definition of personal information. This may make U.S. toy company websites less competitive with other operators. As a practical matter, because computers and mobile devices are often shared in a family, using persistent identifiers, such as IP addresses and UDIDs, could subject users aged 13 and older to COPPA restrictions that would not normally apply. Some adults may know how to clear browser cookies, but many will not know how to clear UDID information stored in mobile caches. The net result will be to impede the user experience, creating frustration for parents and children, and undue burdens on industry that now includes a far greater universe of "operators."

C. No Changes to Photographs, Videos, and Audio Files

Under the 2011 NOPR, the Commission proposed to include photographs, and video or audio files containing a child's image or voice, as "personal information." The FTC does not propose any revisions in this area, and the Supplemental Notice failed to respond to the many concerns raised about including this type of information in the definition. Absent this type of information being linked to other identifiers, the privacy risk is limited.

So long as reasonable methods to assure that the photo, video, or audio file, or facial recognition technology does not include contact details, this sort of engagement does not pose a privacy risk to kids. In addition, TIA reiterates that on adult sites, the mere posting of a picture of a child does not indicate that it was posted by a child. Only where a photograph, video, or audio file is obviously submitted by a child, *and* is associated with other personal information

[20] 77 Fed. Reg. at 46,647.

that would allow the child to be directly contacted online or offline, should this type of information be covered by the COPPA Rule.

IV. SUPPORT FOR INTERNAL OPERATIONS

In the 2011 NOPR, the Commission recognized that information collected by operators for the sole purpose of "support for internal operations of the Web site or online service" – *i.e.*, those activities which are necessary to maintain the technical functioning of the website or online service – should be treated differently than information that is used for broader purposes. In this regard, the FTC proposed to revise the definition of *support for internal operations* so that it includes only "those activities necessary to maintain the technical functioning of the Web site or online service, to protect the security or integrity of the Web site or online service, or to fulfill a request of a child…[and] is not used or disclosed for any other purpose."[21]

Based on comments received that the definition was too narrow to cover the very types of activities the Commission intended to permit – *e.g.*, user authentication, improving site navigation, maintaining user preferences, serving contextual advertisements, and protecting against fraud or theft – the Commission broadened the exemptions for actions that "support the internal operations of a website." While helpful, these changes still do not cover the full suite of activities that should be included.

Further clarity in the definition would be useful to establish that information can be used for market research, product development, intellectual property protection, counting the number of unique visitors, managing traffic, recognizing return visitors across a website or family of websites, and other legitimate business purposes, when such information collected is not used or disclosed to contact a specific individual or for any other purpose inconsistent with support for the internal operations of the website.

V. VERIFIABLE PARENTAL CONSENT

TIA is disappointed that the Supplemental Notice does not reflect a reconsideration of the Commission's proposed elimination of e-mail plus as a mechanism to obtain verifiable parental consent. TIA continues to believe that this has proven to be an effective mechanism to obtain parental consent. The historic distinction between the methods permitted to obtain parental consent reflect a recognition that the greatest risk to children is from exposure to child predators through public posting of personal information that would allow children to be contacted online or offline. The Commission's support for broader filtering techniques to allow children to enjoy an anonymous online experience is consistent with this recognition that collection of personal information for internal marketing purposes simply involves less risk to children's privacy. TIA urges the Commission to retain e-mail plus as a method of consent for internal marketing activities. The alternatives proposed are not likely to be useful, effective, or cost-effective.

[21] 76 Fed. Reg. at 59,810.

VI. SEND A FRIEND E-MAILS

TIA commented in response to the NOPR that it did not view the proposal to alter the FTC's historic view of send a friend e-mails where the activity was consistent with the Commission's FAQs. We ask the FTC to confirm that its outline of accepted ways to allow children to participate in this popular feature has not been altered with the proposed revisions in the NOPR and Supplemental Notice.

VII. REGULATORY BURDEN ESTIMATES

The Commission estimates that some existing operators of websites or online services will be newly covered as a result of the proposed modifications in the Supplemental Notice. The staff, however, failed to adequately assess the regulatory costs and burdens of revisions to the COPPA Rule, and did not fully consider the specific cost and burden estimates previously included in TIA's earlier comments on the NOPR.

In the 2011 NOPR, the Commission asserted that the proposed amendments to the COPPA Rule would impose a one-time burden on existing operators to redesign their privacy policies and direct notice procedures and to convert to a more reliable method of parental consent in lieu of e-mail plus. At that time, the FTC estimated the total burden of complying to be only 60 hours, affecting 2,000 websites. Annualized to 20 hours per year for 3 years, the 2011 NOPR estimated that the burden would be 40,000 hours at a cost of $5,240,000.

Although the Supplemental Notice estimates that there will be approximately 500 existing operators of websites or online services that likely will be newly covered as an operator as a result of the additional revisions, the FTC continues to estimate that the time it takes an existing operator to redesign existing privacy policies and direct notice procedures would be no more than 60 hours. The FTC explains that Nancy Savitt[22] and NCTA[23] were the only commenters who noted that this 60-hour estimate failed to take into account accurate costs of compliance with the Rule. The Commission stated simply that based on these comments, it does not have sufficient information to revise its earlier hours estimate, since these commenters did not provide *empirical* data or specific evidence on the number of hours such activities require. However, the FTC disregarded the empirical economic input that TIA provided in its earlier comments (*see* attached). As illustrated in Table 1, and explained in greater detail below, TIA provided specific hour and labor cost estimates in its comments to the 2011 NOPR, which it expands on below.

[22] Comments by Nancy L. Savitt, No. 00376 (December 21, 2011).

[23] Comments by the National Cable & Telecommunications Association, No. 00338 (December 23, 2011).

Table 1: Comparison of FTC Estimates and TIA NOPR Comments

Costs and Burdens	September 2011 NOPR	TIA Comments	August 2012 Supplemental Notice
Compliance Burden for Existing Operators	60 hours	More than 180 hours	60 hours
Costs for Legal Assistance	$150 per hour	$300 to $450 per hour	$180 per hour
Costs for Technical Assistance	$36 per hour	$72 to $108 per hour	$42 per hour

TIA explained that the disclosure burden for existing operators could be at least *triple* the Commission's estimate, *i.e.*, more than 180 hours. Specifically, TIA stated that:

> …the [FTC's] estimate does not include costs and burdens of "ensuring" security procedures of third parties, securing deletion, managing parental consents, or updating policies to disclose changes in "operators." In addition, the FTC seems to reference only top level domains and, as such, its estimates for implementation of new verifiable parental consent requirements are very low. Each "website" may have many lower level web pages that will be affected by any changes to the parent site. Depending upon the FTC's final revisions to the COPPA Rule, the time it takes to implement technological changes could more than triple the Commission's 60-hour estimate. To implement changes to a website, resources must be devoted to designing, planning, coding, quality assurances, and testing and must be allocated to ongoing operations and maintenance to ensure smooth operation between and among web pages comprising a website. Consequently, costs are likely to be many multiples of the Commission's estimate.[24]

TIA members continue to believe that, on average, compliance costs in year one will be at least 180 hours for external legal and technical support. This is a first-year cost associated with compliance and should not be amortized over three years, as the Commission proposes. In fact, if TIA members are burdened with oversight of agents and service providers to "ensure security" and incorporate the privacy practices of third parties in toy company websites, the burden will be magnified. For a large company with a large marketing department and diverse URLs, services and apps, ongoing costs of managing and updating posted notices and notices to parents, tracking third party compliance, managing consents and security, implementing compliance strategies for new initiatives, and interfacing with a large universe of entities who may now be *operators,* could take ½ of a full-time employee's (FTE) time. In other words, a full-time employee would likely have to devote 50% of his or her time to these compliance activities. This could involve 20 hours per week. The Commission's estimates of the amount of time and hourly fees associated with the greatly expanded compliance burdens are drastically inadequate and well below industry standards.

For example, the 2011 NOPR estimated an assumed labor rate of only $150 per hour for lawyers and $36 per hour for technical personnel. The labor rate for lawyers was based on a

[24] Comments by the Toy Industry Association, No. 00304, at 17-18 (December 21, 2011) (emphasis added).

figure that was roughly midway between the Bureau of Labor Statistics' ("BLS") mean hourly *wages* for lawyers (approximately $54) and what the Commission staff believes more generally reflects hourly attorney costs ($250). Similarly, the $36 estimate of mean hourly wages for computer programmers was also based on the most recent whole-year BLS data. In the Supplemental Notice, the Commission revised slightly the cost estimates for lawyer involvement to $180 and technical labor support to $42. These estimates are still absurdly low and inconsistent with specific cost data previously provided by TIA. Moreover, they are flawed because the Commission has relied on BLS *wage* information to develop estimates of *costs* of compliance. This is only defensible where employees of the operator are directly involved in the compliance effort.

It is improper to rely on BLS statistics for a number of reasons. First, TIA provided *actual cost estimates*, based on a survey of its members, of fees for legal and technical assistance needed to comply with the COPPA Rule. Specifically, TIA explained that its members typically consult with specialized attorneys who understand children's privacy and data security laws. This is a highly specialized area of law, with a relatively few number of experts who are capable of handling it. TIA explained that the *average* rates for engaging lawyers who practice in this specialized area are two to three times the Commission's estimates in the 2011 NOPR, *i.e.*, $300 to $450 per hour. TIA also provided estimates that engaging expert technical personnel can, on average, involve hourly costs that are also two to three times the Commission's estimates in the 2011 NOPR, *i.e.*, $72 to $108.

The Agency cannot ignore specific information about the costs and regulatory burdens provided in comments to the 2011 NOPR. Notice and comment rulemaking procedures obligate an agency to respond to all significant comments, for "the opportunity to comment is meaningless unless the agency responds to significant points raised by the public."[25] The failure to respond to comments is significant as it demonstrates that the Agency's decision was not "based on a consideration of the relevant factors."[26] The Commission's inadequate cost and burden analysis also contravenes the mandate of Executive Order No. 13563 (Jan, 19, 2011) that tasks agencies with reducing regulatory burdens. Specifically, the Executive Order requires agencies "to use the best available techniques to quantify anticipated present and future benefits and costs as accurately as possible." By ignoring empirical data on the *actual* amount of time existing operators will face to comply with the expanded, and *actual* average labor costs for legal and technical personnel previously submitted by TIA, the FTC has failed to comply with the spirit and letter of these requirements.

Second, the BLS statistics relied on by the FTC are based on national *wages*, rather than average hourly billing rates paid for by clients. This is an improper basis on which to base cost estimates. Further, this national average does not reflect regional variation or likelihood that lawyers who practice in such a specialized area of law are more likely to be located in major metropolitan areas. While TIA disagrees that average wages, rather than billing rates, are the correct statistic to use, we note that the FTC has also failed to adopt the best available wage data.

---

[25] *Alabama Power Co. v. Costle*, 636 F.2d 323, 384 (D.C. Cir. 1979) (quoting *Home Box Office, Inc. v. FCC*, 567 F.2d 9, 35-36 (D.C. Cir. 1977)).

[26] *Baltimore Gas and Elec. Co. v. U.S.*, 817 F.2d 108, 116 (D.C. Cir. 1987) (citing *Thompson v. Clark*, 741 F.2d 401, 409 (D.C. Cir. 1984)).

The BLS' most recent Occupational Employment and Wages from May 2011 show that the national estimate of the mean hourly *wages* for lawyers are approximately $64, while estimates for the mean hourly wages are significantly higher in major metropolitan areas, such as the District of Columbia ($77.43), California ($73.27), and New York ($72.63).[27]

In addition, it appears that the BLS statistics do not include law firm partners. These statistics are comprised of full- and part-time workers who are paid a wage or salary, and does not cover those who are self-employed, or owners and partners in unincorporated firms.[28] The average billing rate for lawyers suggested in TIA's comments reflects the fact that high-level partner support is typically required in addressing complex questions of COPPA compliance where external legal support is required. As expected, hourly billing rates paid for by clients are higher than actual wages received by the attorneys, as these costs typically include support staff compensation and other overhead costs. According to *The National Law Journal*'s 2011 annual billing survey, the average hourly firm-wide billing rate (which combines partner and associate rates) ranges from $236 to $633, not taking into account any area of specialization.[29]

Given the specialized nature of children's privacy, TIA's suggested cost estimates are much more realistic than the FTC's estimates. The regional BLS statistics should not be used as a basis to establish cost estimates for external legal support, but can support estimates of the level of in-house legal support likely to be required on an ongoing basis.

Accordingly, TIA urges the Commission to revise its cost estimates to more accurately reflect the hours that will have to be devoted to compliance, and the legal and technical costs associated with compliance, and to apply those estimates to the greatly expanded universe of affected entities. TIA believes that Table 2 better approximates actual costs likely to be incurred in year one. Note that the level of external legal support after year one remains unclear, so these estimates in the chart below are likely low.

[27] *See* Bureau of Labor Statistics, U.S. Department of Labor, *Occupational Employment Statistics, Occupational Employment and Wages, May 2011*; available at: http://www.bls.gov/oes/current/oes231011 htm.

[28] *See* Bureau of Labor Statistics, U.S. Department of Labor, *Occupational Employment Statistics, Frequently Asked Questions (FAQs)*; available at: http://www.bls.gov/oes/oes_ques htm#Ques16.

[29] National Law Journal, "A nationwide sampling of law firm billing rates" (December 2011).

Table 2: First Year Burden Estimates

Costs and Burdens	TIA Estimates
Compliance Burden for Existing Operators (year one)	Minimum 180 hours[30]
Ongoing Compliance Burden for Large, Multi-Site Operators (In-House)	1,040 hours per year
Costs for External Legal Assistance	$300 – $450 per hour
Costs for Technical Assistance	$72 – $108 per hour
Costs for In-House Legal Support	$64 - $72.95 per hour[31]

A reasonable estimate of the costs for a large firm with multiple URLs, apps, and services in year one is $31,200 – $46,800 for external legal and technical support, plus $66,560 - $75,868 for in-house legal support. As is apparent from this data, the actual year one compliance burden is expected to be many times higher than the Commission's estimates. While additional external legal and technical support will likely be required in following years, those costs are not included in this chart.

VIII. CRITICAL POINTS THAT THE FTC HAS FAILED TO ADDRESS

The Commission is not proposing to alter some aspects of the earlier NOPR criticized by TIA and others in comments. As discussed in these comments, TIA identified serious concerns with designating a photograph, video, or audio file containing a child's image or voice as *per se* personal information, even when no actual personal information is linked to the photograph, video, or audio file. E-mail plus presumably remains barred under the revised proposed rule, even though the Commission apparently accepts the reliability of a child entering his or her age for age-screening purposes, as do we. The Commission has not provided further examples of practical ways to obtain verifiable parental consent. Furthermore, provisions requiring that operators "ensure" that agents comply with COPPA have not been changed.

These earlier proposed revisions, coupled with the most recent changes, will continue to present practical, technical, and operational challenges to the operator if the FTC fails to revise them. TIA attaches and incorporates by reference its prior comments to the 2011 NOPR, and urges the Commission to further consider TIA member concerns in these areas.

CONCLUSION

The privacy of all our consumers is of central importance to TIA and its members. The COPPA Rule has been effective in protecting children since its inception. 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 full extent of all costs and benefits associated with these proposed revisions must

[30] TIA assumes conservatively that at least 80 hours of external legal support and 100 hours of technical support will be required in year one.

[31] Since many businesses are based in California and New York, the range of in-house legal costs includes the BLS average plus the average BLS wage statistics for lawyers in California and New York.

be weighed to avoid any unnecessary and unintended adverse effects on both consumers and on companies that must comply. As a strong advocate for children, and a staunch supporter of consumer privacy, TIA and its members appreciate the opportunity to submit these comments to the FTC's proposed, further modifications to the COPPA Rule, and looks forward to an ongoing dialogue with the Commission on practical approaches to enhance children's privacy, while assuring that toy companies can continue to offer engaging content for children.

Respectfully submitted,

Carter Keithley
President

Of Counsel:
Sheila A. Millar
Crystal N. Skelton
Keller and Heckman LLP

ATTACHMENTS

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	**)**	
Proposed Revisions to the	**)**	
Children's Online Privacy	**)**	
Protection Rule, Project No. P104503	**)**	

COMMENTS OF THE TOY INDUSTRY ASSOCIATION

December 21, 2011

In the Matter of

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

COMMENTS OF THE TOY INDUSTRY ASSOCIATION

INTRODUCTION

The Toy Industry Association ("TIA") is pleased to submit these comments in response to the Federal Trade Commission's ("FTC" or "Commission") request for public comment on its proposed amendments to Children's Online Privacy Protection Rule ("COPPA Rule"), promulgated under authority of the Children Online Privacy Protection Act ("COPPA").[1] The FTC is requesting comments on proposed modifications to five major areas, including definitions, notice, parental consent, confidentiality and security of children's personal information, and safe harbor programs, and provides new guidance for data retention and deletion. TIA's members have a strong commitment to privacy in general, and to children's privacy in particular. The proposed rules include some useful revisions that will facilitate our members' ability to offer fun, safe online environments for children. However, the proposed rules also fundamentally change some long-standing policies which have proven to be protective of children's privacy by (1) eliminating the common-sense distinction between personal and non-personal information, (2) restricting the ability to use anonymous data for research, and (3) eliminating a useful and widely-accepted method of parental consent. Our comments therefore also address areas where we disagree that the Commission has struck the appropriate balance between protecting privacy and creating undue costs and burdens.

BACKGROUND

TIA is recognized by governments, 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 550 member companies that account for more than 85 percent of the U.S. domestic toy market. 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.

Safeguarding children and earning the trust of parents are central to our members' businesses. Thus, toy companies, for more than a decade, have not only created fun, safe toys for children, they have offered entertaining, educational, and safe online environments for kids. However, toy companies view parents and teens to be an important audience. Many TIA

[1] 76 Fed. Reg. 59,804 (September 27, 2011).

members host websites that offer online content for teen and adult collectors, online stores where parents can shop, and apps for general audiences or families. The privacy of all consumers is thus an important value to TIA member companies. In fact, even before the enactment of COPPA, TIA as an institution, and individual members of TIA, supported strong self-regulatory measures to protect children's privacy through the Children's Advertising Review Unit ("CARU"). The requirements of COPPA were largely based on the pioneering work on children's privacy at CARU. Privacy protection for children has been predicated on several core principles: the collection of personal information that allows a child to be directly contacted online or offline should be limited; parental consent should be obtained where more than a limited amount of such information is collected; and public disclosure of a child's personal contact information poses substantially greater risk than internal marketing. Our industry remains committed to making sure that sensible children's privacy rules reflect changing technology as well as practical business realities that reflect these core principles. To this end, TIA previously submitted comments in response to the FTC's request for public comment on the implementation of the COPPA Rule in June 2010.2

TIA continues to believe in finding new and better ways to protect the safety and privacy of children, and appreciates the opportunity to provide comments on the FTC's proposed revisions to the COPPA Rule. These comments reflect our members' longstanding experience with adhering to COPPA requirements, and address legal, policy, operational and practical aspects of the existing COPPA Rule and implications of possible revisions.

EXECUTIVE SUMMARY

TIA fully supports the Commission's periodic review of all of its rules, including the COPPA Rule. We agree that technological changes in the digital environment, as well as market developments, merit this review. Importantly, the FTC has not identified significant risks to children's privacy posed by the existing framework. TIA agrees with the Commission that:

- The statutory definition of a "child" remains appropriate.[3] COPPA's parental notice and consent model works well for younger children, and teens have increased constitutional rights to obtain information and express themselves publicly.
- The "actual knowledge" standard should be retained for those sites or online services not directed to children under 13.
- Date of birth, gender or zip codes do not constitute personal information.
- We support the proposed modifications in rule language are needed to confirm that filtering and other technology is an appropriate way to safeguard children's privacy while offering them the expanded ability to engage in social interactions increasingly of interest to them.

[2] *See Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection* Rule, 75 Fed. Reg. 17,089 (April 5, 2010); Comments of the Toy Industry Association, Inc., No. 547597-00031; available at: http://www.ftc.gov/os/comments/copparulerev2010/547597-00031-54843.pdf.

[3] 15 U.S.C. § 6501(1).

- We agree that a parent's e-mail address can be collected for purposes of notifying the parent about a child's activities at a website.

TIA disagrees, however, with some of the fundamental changes the FTC has proposed. These changes are not necessitated by evidence of privacy or security risks to children, but will exponentially increase the burdens of COPPA compliance for website operators, service providers, children and parents alike.

- FTC broadly defines "online services." While we agree that a variety of online services could be covered, we also agree that SMS and MMS services fall outside the statutory definition. However, we are concerned that the proposal has not adequately considered the internal processes and procedures that companies will be required to take to ensure that these services now comply with all COPPA requirements.

- Redefining "personal information" to include information previously deemed anonymous has potentially broad implications, and the Commission's suggestion that the scope of these sweeping changes is limited to children's sites is disingenuous. FTC's proposed changes could limit the ability of TIA member companies to offer certain content, conduct appropriate research, and engage in marketing to parents consistent with current advertising technologies. More troubling still is that the changes are not based on any evidence that companies are "tracking" children across the Internet for online behavioral advertising purposes. The proposed revisions will likely impose broader burdens on operators to obtain parental consent that will adversely affect the ability of operators to offer fun, safe, and anonymous activities for kids, and to analyze interest in their sites. Further, the toy industry will be at a competitive disadvantage to other industries that target a broader demographic, such as movies and videogames, that reaches kids, teens, and young adults, and are not subject to the same strict interpretation of "personal information."

- The proposed definition of "support for internal operations" is too narrow, especially considering the proposed expanded definition of personal information. Data sharing with affiliates and business partners for traffic management, counting unique visitors, and conducting market research has been a traditional part of the online landscape for years with no indication that the privacy of children is adversely affected. It will also limit the ability of toy companies to offer common registration options across their family of websites.

- The proposed modifications to online and direct notices do not materially improve the quality of notices. Requiring identification of all operators is burdensome, may impede upon commercial relationships, and could require frequent updates to online notices as business partners change. Further, FTC should not modify notice requirements to mandate posting a link to the online notice in any location where mobile apps can be purchased or downloaded.

- The Commission should not eliminate the "e-mail plus" method as a means of obtaining parental consent for internal use. Similar cost-effective and efficient technologies to replace this method have not yet been developed and those proposed

by the Commission are costly and privacy-invasive. Any new methods proposed under the safe harbor approval process are unlikely to provide practical alternatives since FTC has already rejected a majority of them.

- FTC needs to provide additional guidance on what it means to ensure that reasonable procedures are in place to protect the confidentiality, security, and integrity of personal information. Operators regularly investigate agents, service providers and business partners to ensure that they will responsibly maintain the security and confidentiality of children's data, but cannot be the guarantors of security measures by third parties. So long as operators conduct reasonable due diligence into third party security measures, they should not be liable under the proposed Rule.

- The proposed Rule will increase compliance burdens. The FTC's cost estimates of the burden to comply with the revised rules as proposed are grossly understated, some costs are not included, and the Commission has not evaluated the potential burdens on parents associated with handling new verifiable consent methods and the possibility of multiple privacy notices reflecting what may now be considered to be a "material change" in privacy policies.

COMMENTS

TIA believes that the COPPA Rule has worked well to protect children's online privacy. Revisions to the COPPA Rule should not be made lightly. They must offer substantial privacy and safety benefits to both children and their parents without placing undue burdens on operators. TIA members are therefore deeply concerned that elements of the proposed revisions to the COPPA Rule will in fact undermine the goals of COPPA and impose significantly greater burdens on operators and service providers. The FTC has proposed a series of modifications and is soliciting comments on several important questions. We provide below our comments on issues of most interest to TIA members.

I. SCOPE

TIA agrees that the age of a child for COPPA purposes could not be changed under the statute. Moreover, TIA concurs that any effort to expand the scope of COPPA to cover teens would impermissibly burden constitutional rights. TIA also concurs that only websites or online services directed to children, or those with actual knowledge that they are dealing with children under 13, are covered by COPPA. A general interest site, like an e-commerce site or a site for collectors or families, is not directed to children under 13. This is an important distinction to toy companies that offer online stores and adult or general family offerings. The Commission should make clear that sites that may be linked to a child-oriented site or service are not within the scope of COPPA, absent actual knowledge.

Neither COPPA nor the Rule defines the term "online service." The FTC proposes that the term "online service" covers "any service available over the Internet, or that connects to the Internet or a wide-area network."[4] Under this notion, the Commission broadly views mobile applications ("apps"), Internet-enabled gaming platforms, voice-over Internet Protocol ("VOIP")

[4] 76 Fed. Reg. at 59,807.

services, geolocation services, premium texting, and coupon texting programs (internet to mobile) as covered by the COPPA Rule.

TIA agrees that a wide variety of online services may be covered, excluding mobile and SMS communications as a statutory matter. However, we are concerned that the proposed rule does not fully consider the additional internal processes and procedures that will have to be deployed to ensure that all services that might conceivably be considered "online services directed to children" comply with all COPPA requirements.

To the extent that COPPA is applied to other technologies currently deemed to fall outside of COPPA, aspects or limitations of these technologies would require further revisions to the Rule in ways that cannot be implemented consistent with current statutory authority. For example, we agree that the Commission does not have authority over MMS and SMS. At the same time, parental controls for mobile media, coupled with the fact that parents make the ultimate decision on whether to purchase and let their child use a cell phone, provide parents with the ultimate choice on whether these types of mobile services are appropriate for their child. Because the Commission has indicated that it lacks authority to permit use of text messages to a parent's cell phone number as a vehicle to offer notice or consent,[5] exclusion of MMS and SMS messaging avoids applying overly restrictive barriers to use of the technology. Technological limits on the ability to offer online or direct notices or obtain parental consent will have cost impacts that we address more specifically in Section IX.

II. ACTUAL KNOWLEDGE STANDARD

Retention of the actual knowledge standard is required by the statute,[6] but also makes practical sense. The distinction is important to TIA members, many of whom operate adult-oriented collector or e-commerce sites. The collection of data at these sites is presumed to relate to an individual over 13, and we agree that there is no basis to impose an imputed knowledge standard.

Similarly, many apps may be targeted to the nostalgia consumer, or appeal to general audiences. Simply because an app features a beloved toy character does not automatically mean it is targeted to children.

III. DEFINITION OF PERSONAL INFORMATION

The types of information currently defined under COPPA and the COPPA Rule as "personal" are those that would allow an individual child to be physically contacted directly by a website operator or online service provider that either operates a website directed to children or has actual knowledge that they were dealing with a child. The Commission proposes to redefine the term "personal information" to include data it previously deemed anonymous, including screen or user names, persistent identifiers, geolocation information, photographs, video, and

[5] 76 Fed. Reg. at 59,817.

[6] 15 U.S.C. § 6502(a)(1)

audio files, and any information combined with an item of personal information is personal information.[7]

TIA members' websites and online services directed to children have been built in compliance with the COPPA Rule and CARU Guidelines. This means that unless information like an IP address, screen name, or the like is linked to information that allows a child to be directly contacted, such as via an e-mail address, it is deemed anonymous. The COPPA statute protects individual privacy and does not accord privacy rights to machines or devices. The proposed Rule thus upsets more than a decade of good privacy practices grounded in the statutory framework that have earned the trust of parents. The new framework of privacy proposed by the FTC will likely confuse parents as disclosures and consent will be required in connection with data that parents today do not commonly understand to involve "the release of personal information collected from a child *in identifiable form*".[8] Parental consent would need to be obtained in many cases for internal marketing, web analytics and similar activities. Companies may have to solicit more personal information from parents and children than under the current model, creating greater obstacles to allowing children to freely and anonymously engage in website content and activities and confusing parents who trust that TIA members do safeguard their children's privacy.

The Commission requests comment on the impact and limitations of defining personal information to include certain information currently deemed to be anonymous. We address the issues related to redefining screen or user names, persistent identifiers, identifiers linking children's activity across different websites, the combination of date of birth, gender, and zip codes, or ZIP+4, photographs, video, and audio files, and geolocation information as personal information immediately below.

*A. Screen or User Name*s

Offering children the ability to enjoy online activities anonymously is central to many TIA members' kid-directed websites and online activities. TIA members offer opportunities for children to participate by registering an anonymous user and screen name. They collect limited information, like first name and an e-mail address, to respond to a one-time request, and have successfully adopted e-mail plus as a method of consent for internal marketing, whereas more information, like a home address, is necessary to award a prize or engage in other activities. Maintaining anonymity of children and avoiding the collection of more information than necessary to allow a child to participate in a website or online activity is an important tenet of COPPA, one that toy companies have embraced. Many toy company sites are structured to collect only a user name and password to personalize the visitor's experience or recall a users' favorite area of the site without collecting personal information.

A user name and password may relate to a "specific individual," but, unlike an e-mail address, 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 and permits companies to appropriately evaluate interest in its sites and offerings. The user name and password may be

[7] 76 Fed. Reg. at 59,810-59,813.

[8] 15 U.S.C. § 6501(4).

linked to an IP address to facilitate the user experience, including allowing the user to sign in on other websites within the family of companies. The Commission should not include a screen or user name in the definition of personal information if the screen or user name does not reveal an individual's e-mail address or identity. If screen and user names are considered to be personal information, the result will be to potentially require TIA members to eliminate their entire database of anonymous registration information when a new rule is finalized, an outcome that is undesirable from a privacy standpoint, and one that will be costly to companies that have abided by the COPPA Rule. It also would mean that any data points linked to a screen or user name, whether a picture that otherwise lacks identifying personal information, or an IP address, is redefined as personal information, requiring parental consent.

Toy companies are mindful that the greatest potential privacy risk to children relates to the possible public disclosure of information that allows them to be directly contacted online or offline. We support obtaining verifiable parental consent using robust measures in such circumstances. We are also pleased that the Commission recognizes that filtering techniques can be effectively applied to allow children to engage in social activities at child-oriented websites anonymously without compromising privacy. We support this change and agree that it might be a way to offer added social engagement for children at sites that are truly appropriate for kids.

B. Persistent Identifiers

The Commission also proposes to include persistent identifiers (*i.e.*, customer number held in a cookie, IP address, processor or device serial number, or unique device identifier) in the definition of personal information if used for functions other than or in addition to support for the internal operations of the site or protecting security.[9] The Commission equates persistent identifiers to a home address or phone number, which is considered personal information.[10] Unlike a home address or phone number, where a child could be directly contacted, an operator has no way of contacting anyone directly from a persistent identifier.

Several U.S. courts have already found that IP addresses, for example, do not constitute personal information, because an IP address only identifies a computer.[11] These decisions are

[9] 76 Fed. Reg. at 59,810.

[10] *Id.*

[11] *See e.g., In re Application of the United States of America for an Order Pursuant to 18 U.S.C. §2703(d)*, Nos. 11-DM-3, 10-GJ-3793, 11-EC-3, *6-7 (E.D. Va., Nov. 10, 2011) (Memorandum Opinion) ("IP address information, by itself, cannot identify a particular person…IP address information can identify a particular personal computer, subject to the possibility of dynamic addressing…but it can also identify a device that connects to another network, such as an internal home or office network. Moreover, though IP addresses can assist in identification, they have been found inadequate to identify a particular defendant for the purposes of service of process…Even if certain actions are traceable to an IP address, therefore, attributing those actions to a real person requires evidence associating a real world person with the residuum of his more transient and diaphanous presence in cyberspace"); *Klimas v. Comcast Cable Comm'cns, Inc.*, 465 F.3d 271, 276 n.2 (6th Cir. 2006) ("We further note that IP addresses do not in and of themselves reveal 'a subscriber's name, address, [or] social security number.' That information can only be gleaned if a list of subscribers is matched up with a list of their individual IP addresses"); *Columbia Pictures Indus. v. Bunnell*, No. 06-1093, at *3 n.10 (C.D. Cal. May 29, 2007) ("As an IP address identifies a computer, rather than a specific user of a computer, it is not clear that IP addresses . . . are encompassed by the term 'personal information' in defendants' website's privacy policy"); *Johnson v. Microsoft Corp.*, No. C06-0900RAJ (W.D. Wash., June 23, 2009) ("In order for 'personally identifiable information' to be personally identifiable, it must

consistent with the FTC's longstanding interpretation. The proposed redefinition of personal information does not account for the fact that, although some Internet service providers assign static IP addresses that remain constant with regard to a particular device, most households with young children use shared computers. Particularly when it comes to households with children, a device does not generally identify a specific individual or user of the device. Some ISPs continue to assign dynamic IP addresses that change each time the user connects to the Internet. A dynamic IP address may never be used again by the same computer. Consistent with its prior comments on the topic, TIA continues to have grave reservations about the Commission's proposal to redefine IP addresses and other persistent identifiers as "personal information."

The Commission also proposes that parental notification and consent prior to the collection of persistent identifiers is required where this information is used for purposes such as gathering data on a child's online activities or behaviorally targeted advertising to the child. To the extent the FTC proposes to now bar routine web analytics, there is no factual basis to prohibit companies from utilizing technological tools to understand visitors. To the extent the proposal is predicated on the concern about third party tracking for online behavioral advertising ("OBA") purposes, again, there is no factual support suggesting that this is occurring. The Network Advertising Initiative's ("NAI") 2010 Annual Compliance Report confirmed that when it comes to cookies used for OBA "[n]one of the evaluated members were found to create segments specifically targeting children under thirteen, and NAI staff's review revealed no compliance deficiency with respect to this provision of the Code. The member companies have processes and procedures in place to ensure that segments specifically targeted at children under thirteen are not created or used."[12] The NAI Code prohibits the use of personally identifiable information ("PII") or non-PII to create OBA segments specifically targeted at children under 13 without verifiable parental consent. The Commission's record suggests that OBA-targeted advertising to children is a theoretical issue, and not an actual issue. In this regard, the FTC should take into consideration self-regulatory efforts already in place that govern the use of OBA towards children.

C. Identifiers that Link Activity Across Different Websites

The FTC is considering whether an identifier that "links the activities of a child across *different* websites or online services" should be considered personal information.[13] Although this is intended to serve as a catch-all category to cover the online collection of information about a child over time for the purposes of either online profiling or delivering behavioral advertising to that child, the term "different" in this context is not clearly defined. Does the definition mean any website outside of an initial domain, implicating links between affiliated websites, or does it mean third-party websites? If a user visits a website and, from that website, visits additional websites or web pages (perhaps with different products or other offerings)

---

identify a person. But an IP address identifies a computer, and can do that only after matching the IP address to a list of a particular Internet service provider's subscribers").

[12] Network Advertising Initiative, *2010 Annual Compliance Report*, February 18, 2011; available at: http://www.networkadvertising.org/pdfs/2010_NAI_Compliance_Report.pdf.

[13] 76 Fed. Reg. at 59,830 (to be codified at 16 C.F.R. § 312.2) (emphasis added).

within the initial websites' ecosystem, will that prohibit the use of website analytic tools attached specifically to a visitor of a specific website?

A toy company may operate several different websites outside of its initial domain, but that are still in the "family" of websites owned by the operator. It is unclear in this regard, whether the FTC is proposing that an identifier that links the activities of a child outside of an initial domain to a related website is considered personal information, or whether the FTC is referring solely to the identifier that links the activities of a child across third-party websites operated independently of a corporate family of companies and in a manner unrelated to providing services to the parent or affiliate. Such an expansive definition could prevent toy companies from utilizing the most up to date tools to target adult purchasers. The definition could also potentially bar toy companies from offering visitors the ability to use common anonymous screen names and passwords across a family of websites, or sharing market research, web traffic or similar information across members of the same corporate family. Toy companies must be able to utilize ad tracking software, including beacons, pixels, and web analytic tags. The collection of this type of data is anonymous and is aggregated to measure and analyze consumer habits and characteristics, whether or not stored in a database managed by a company that provides analytical services or by the companies themselves. These tools, for example, allow a website operator to measure the total outreach, behavior, and use of the website by its visitors without identifying a specific individual. In turn this data may support product development efforts. None of these activities appear to fall within the Commission's proposed narrow definition of "support for the internal operations of the website or online service."

Many TIA member companies also operate e-commerce websites which are adult directed but linked from a children's website. To continue utilizing these basic means to understand information about its site visitors, and click-through visitors, the rules must be clear that an adult collector or e-commerce site is not directed to children merely because a visitor may link from a child-directed area.

D. Date of Birth, Gender, and Zip Codes

TIA agrees with the Commission's conclusion that date of birth, gender, and zip codes (including zip plus 4) alone are not personal information. The FTC, however, requests comment on whether the combination of such information is enough to permit the contacting of a specific individual such that this combination should be included in the COPPA Rule as "personal information." This type of demographic information merely helps identify categories of visitors to help with product and site development and related market research, information that is critically important to ongoing innovation in the toy industry. Zip codes can be used to send out general mailing to households in a general geographical location or for general marketing purposes. This type of information helps companies understand their general target audience without identifying a specific individual.

E. Photographs, Video, and Audio Files

The FTC proposes to include photographs, and video or audio files containing a child's image or voice, as personal information. For a child to post a photo or video poses a risk only when combined with other information that may enable the physical or online contacting of a

child.[14] So long as reasonable methods to assure that the photo, video, or audio file, or facial recognition technology, does not include contact details, this sort of engagement does not pose a privacy risk, and association with a screen or user name that remains anonymous should be permitted. This is an example where filtering techniques, as proposed by the Commission, may prove useful. In addition, on adult sites, the mere posting of a picture of a child does not indicate that it was posted by a child; only where there is some actual knowledge that the photograph was submitted by a child should this be covered.

F. Geolocation Information

To the extent geolocation information identifies an exact address (house number, street, city, state), it is equivalent to a home address and is currently covered by COPPA where a website or online service is directed to children. Generally we do not understand geolocation information to be so precise. Geolocation initiatives in any event are typically targeted to adults or general audiences, where the actual knowledge standard applies.

III. SUPPORT FOR THE INTERNAL OPERATIONS

Under the proposed Rule, the Commission proposes to exclude certain persistent identifiers from the definition of personal information when used to support the internal operations of the site or protect security. The Commission views the phrase "support for the internal operations" as permitting operators' use of persistent identifiers for purposes such as user authentication, maintaining user preferences, service contextual advertisements, and protecting against fraud or theft. FTC is requesting comment on whether this limitation is sufficiently clear to provide notice of the circumstances under which a persistent identifier is not covered by the COPPA Rule.

The FTC's proposed definition of "support for internal operations" is too narrow, especially considering the proposed expanded definition of personal information. The DAA's newly released *Self Regulatory Principles for Multi-Site Data* provide a better definition of activities that support internal operations of a website or online service,[15] and the FTC should adopt this definition. Internal operations include market research, product development, and the collection of data for operations and system management purposes, including: (1) intellectual property protection; (2) compliance, public purpose and consumer safety; (3) authentication, verification, fraud prevention, and security; (4) billing, product or service fulfillment; (5) delivery of online content, advertisements or advertising-related services using reporting data; and (6) reporting (*i.e.*, the logging of data on a website or the collection or use of other information about a browser, operating system, domain name, date and time of viewing of the webpage or advertisement, or impression information for statistical reporting in connection with the activity on a website, web analytics, optimization of location ad and media placement, reach and frequency metrics, ad performance, and logging the number and type of advertisements served on a particular website). Internal operations also include counting the number of unique visitors, managing traffic, and recognizing return visitors across a family of sites. Further,

[14] 76 Fed. Reg. at 59,813.

[15] Digital Advertising Alliance, *Self Regulatory Principles for Multi-Site Data* (November 2011); available at: http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.

market research and product development, or instances where the data will be deidentified within a reasonable period of time, also fall within the support of the internal operations of the site or service.

The FTC should make clear in a revised definition outlined above that collecting the kind of information listed above through the use of persistent identifiers constitute "support for the internal operations." Collection of such information allows site operators to accurately assess internal operations and costs associated with the different functionalities of their websites or online services. Barring such action absent parental consent would fundamentally alter current business practices, imposing extensive costs and burdens and impinging on the ability to conduct business, all without any evidence that these activities, which occur today and are perfectly consistent with COPPA, create privacy risks to children.

IV. NOTICE

The FTC proposes several changes to online notices and direct notices to parents. The Commission's objectives in this area are to reinforce COPPA's goal of providing complete and clear information in the direct notice, and to rely less heavily on the online notice or privacy policy as a means of providing parents with information about operators' information practices.[16] TIA and its members appreciate the Commission's attempt to streamline the placement and content of notices that operators must provide, but the proposed changes do not achieve the objective of streamlining notices to parents. In particular, the Commission proposes to require operators to provide contact information for *all* operators of a website in the online notice (including each operator's contact information), rather than designating a single operator as the contact point.[17] Attention must also be given to new platforms that the FTC now defines as falling within the scope of COPPA, including mobile apps. Companies that have not developed websites that are WAP-enabled (for mobile) or otherwise optimized for technological platforms not previously covered under COPPA will face technical challenges and could incur significant costs in making notices available on these additional platforms, and may also have difficulty in offering direct notices to parents and obtaining consent.

The combination of the overly expansive definition of "personal information" and overly narrow definition of "support for the internal operations" may now require that entities currently deemed agents and services providers who support the internal operations of the website or online service, or even other brands or affiliates of a parent company, are now themselves "operators." The net result will be that companies offering websites or online services to children may have to update their online privacy policies periodically each year to reflect work with different operators over the course of time. While the FTC has not addressed this issue, it is assumed that revising a privacy policy to indicate a change in the identity of an "operator" constitutes a "material change" requiring renewed notice and consent from users. This change imposes new costs and burdens on companies offering kid-directed online services or websites. This will be a burden on business to provide, but also a burden on parents to receive. This could implicate affiliate data-sharing as well as sharing with service providers or promotional partners.

[16] 76 Fed. Reg. at 59,815.

[17] *Id.*

Similarly, operators should not be required to post a link to their online notice in any location where their mobile apps can be purchased or otherwise downloaded. Changing commercial relationships may make keeping up with changing distribution outlets challenging, and again result in frequent updates if these changes are considered to be a "material change" to the privacy policy.

V. VERIFIABLE PARENTAL CONSENT AND EXCEPTIONS

COPPA requires operators of children's websites or online services to obtain verifiable parental consent when seeking to collect, use, or dispose of personal information from a child outside some narrowly crafted exceptions. The FTC has approved a sliding scale of methods of obtaining consent that have worked well to protect children's privacy and safety, while allowing operators to effectively and efficiently obtain the necessary parental consent required by COPPA. The sliding scale approach has been grounded in the FTC's recognition that interactions with a family of branded websites, where limited personal information is collected and used for internal marketing by the company or brand, and is not shared with third parties or publicly disclosed, poses significantly lower privacy risks than public disclosures. The Commission, however, proposes to eliminate the "e-mail plus" method as a means of obtaining parental consent for internal use after previously determining that e-mail plus should be extended indefinitely.[18]

During the June 2010 roundtable discussion of COPPA, several participants, including one from the FTC, remarked that technology similar to email-plus has not yet been developed.[19] TIA and many other organizations urged the FTC to retain e-mail plus as a viable means of obtaining parental consent.[20] Similar cost-effective and efficient technology has not yet been developed to replace the e-mail plus system.

---

[18] *Children's Online Privacy Protection Rule*, 71 Fed. Reg. 13,247, 13,257 (March 15, 2006).

[19] *See* Transcript of the COPPA Rule Review Roundtables, pp. 213 (June 2, 1010) (A FTC representative stated that e-mail plus "was supposed to be a very temporary solution, and we extended it, because we didn't come up with other technological choices that worked with the same ease as email-plus, and then we ultimately, in our 2007 report, said that email-plus would be a permanent standard for the foreseeable future"); available at: http://www.ftc.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf.

[20] *See, e.g., Comments by the Direct Marketing Association, Inc.*, No. 547597-00072 ("This sliding scale approach has proven to be a sound approach to protecting children online"); *Entertainment Software Association*, No. 547597-00048 ("The ESA supports the COPPA Rule's 'sliding scale' approach of requiring one level of verifiable parental consent for internal uses and a higher level where a child's personal information will be disclosed to others"); *Motion Picture Association of America*, No. 547597-00078 ("MPAA members use a variety of mechanisms to secure verifiable parental consent under the sliding scale, which permits businesses to identify cost effective mechanisms to secure parental consent that are appropriately tailored to a particular setting."); *Promotion Marketing Association*, No. 547597-00066 ("The COPPA Rule currently allows for so-called 'e-mail plus' verification. This method weighs practicality and safety and recognizes that e-mail is the primary way we communicate today and gives parents a tool they can easily use. At the same time, the 'plus' aspect provides a reasonable safeguard no more vulnerable to manipulation or circumvention than the neutral age gating that is used to exclude children from content and activities… This method should not only be retained, but expanded to allow for external sharing and use if specifically and clearly disclosed in the notice and request to the parent."). Comments available at http://www.ftc.gov/os/comments/copparulerev2010/index.shtm.

The FTC is proposing to eliminate e-mail plus on grounds that it has impeded the development of more reliable methods of obtaining verifiable parental consent. Ironically, while apparently relying on the honesty of children to provide an e-mail address of a parent for purposes of direct notices to parents, the Commission now inconsistently says that the same addresses identified by children and accepted as accurate for purposes of requiring companies to send notices to parents cannot be used to obtain the type of additional information used only for internal marketing permitted pursuant to e-mail plus. At the same time, the FTC has not identified a cost-effective digital alternative to e-mail plus. Instead, the FTC is proposing a new process to review and consider alternative means of "verifiable parental consent." Having rejected options such as digital signatures, text messaging, parental control technology and other methods, it is not likely that new low-cost, efficient methods of parental consent will soon be approved.

The Commission proposes to recognize several additional methods for obtaining verifiable parental consent, but these methods do not provide a more affordable or efficient means to obtain consent. The first method allows for submission of electronically scanned versions of signed parental consent forms; the second allows for use of video verification methods. Economic conditions for some families preclude ownership of a scanner or the technology for video conferencing, thereby negating the effect of parental consent in these areas. Technology "know-how" gaps may also preclude some parents from using scanners or video conferencing methods, even if available. More importantly, non-automated technology will require dedicated employees to review, verify, and input each scanned parental consent form or video feed into a database management system, potentially requiring companies to gather literally millions of forms based on new definitions of personal information, limited exclusions for support for the internal operations of a website, and revisions to notices requiring identification of individual "operators." While TIA believes that all potentially reliable methods should be recognized, these proposed methods do not provide a viable substitute for e-mail plus and banning e-mail plus will exponentially increase compliance costs.

The Commission also proposes allowing operators to collect a form of government-issued identification, such as a driver's license or last four digits of a social security number, from the parent in order to verify parental consent.[21] It is highly unlikely that a parent will provide this type of information to an operator for the purpose of allowing a child to visit and/or use its website services and offerings. Online guidance to consumers uniformly urges them to use extreme caution before sharing a Social Security number, drivers' license, or similar information online due to risks of identity theft. In addition, collecting this type of information requires companies to handle highly sensitive personally identifiable information, increasing the burden on companies of employing a higher level of data protection and security measures and increasing potential liability in the event of a breach incident. In fact, the FTC has recommended that use of Social Security numbers to authenticate an individual's identity be limited.[22]

[21] 76 Fed. Reg. at 59,818.

[22] See Security in Numbers: Social Security Numbers and Identity Theft: An FTC Report on Social Security Number Use in the Private Sector, December, 2008, available at http://www.ftc.gov/opa/2008/12/ssnreport.shtm.

Similar cost-effective and efficient technologies to replace e-mail plus have yet to be developed. Allowing scanned parental consent forms or video conferencing can be costly to operators, and consent may not be obtained before the child loses interest. Submittal of government identification such as Social Security numbers or drivers licenses as proof of consent is privacy-invasive. It requires operators to unnecessarily collect sensitive personal information and expands use of these identifiers as an authentication method contrary to prior FTC recommendations. Any new methods proposed under the safe harbor approval process are unlikely to provide practical alternatives since the FTC has already rejected a majority of new technologies, including text messages, digital signature and parental controls in gaming consoles.

The e-mail plus mechanism relies on the submittal of a parent's e-mail address from a child to send notices and obtain consent. Generally TIA members ask a child to provide a separate e-mail address of a parent where both the child's e-mail address and the parent's e-mail address is sought to provide added confidence that notices and requests for consent are sent to parents. To the extent the FTC is encouraging broader use of parental notices, websites directed to children will still have to rely on a child to provide an accurate e-mail address of his or her parent. The proposal offers no explanation of why a website can rely on e-mail addresses of a parent provided by children to send the direct notice to parents, but cannot rely on the same e-mail addresses to request that parents provide the additional information required to allow a child to participate in activities that constitute internal marketing under the "sliding scale" consent mechanism. E-mail plus remains especially important to the toy industry, and TIA urges that it be retained.

At the same time, we support an expedited process to review new verifiable consent mechanisms. This will provide more information on possible alternatives. However, since the Commission has already rejected a variety of suggested methods, we have no confidence that new, easy-to-use methods will be approved quickly enough to minimize the burden of switching to other methods designated by the FTC in its proposal. Until such time as more practical methods of verifiable parental consent have actually been approved, the Commission should continue to allow e-mail plus to be used.

Although not explicitly addressed in either the COPPA rule or the proposed revisions, TIA does not understand that the FTC's proposed revisions to the COPPA Rule will change how the FTC treats "forward-to-a-friend" e-mails per FAQ 44.[23] Send a friend e-mails have always been extremely popular with children from the earliest days of the Internet. Child-directed websites have always been able to collect a recipient's e-mail address (and, if desired, a sender and/or recipient's first name and last initial) for purposes of sending an e-mail at the request of a child, consistent with COPPA, even absent an explicit exception. In this context, the operator is acting as a carrier or ISP in transmitting the message. This exception applies so long as the e-mail does not permit the sender to enter the sender's full name or email address, or the recipient's full name. The proposed revisions permitting reasonable filtering and screening may be helpful in expanding social networking options by allowing kids to develop their own messages in send a friend e-mails so long as the name or e-mail of the requesting child does not appear in the "from" line of the message.

[23] *Frequently Asked Questions about the Children's Online Privacy Protection Rule*, FAQ #44 (Rev. October 7, 2008); available at: http://www.ftc.gov/privacy/coppafaqs.shtm.

VI. CONFIDENTIALITY AND SECURITY OF CHILDREN'S PERSONAL INFORMATION

The Commission proposes amending the COPPA Rule to add the requirement that "operators take reasonable measures to *ensure* that any service provider or third party to whom they release children's personal information has in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information."[24] It is not clear what FTC means by the word "ensure." Operators regularly investigate agents, service providers, and business partners to assure that they will responsibly maintain the security and confidentiality of children's data, but are not guarantors of third party actions. Requiring companies to go beyond reasonable due diligence – for example, by effectively mandating auditing third-party processes – would impose undue burdens on website operators. TIA requests that the Commission clarify what procedures operators would need to have in place to ensure that a service provider or third party has reasonable measures in place.

As previously indicated, 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. TIA members operate their websites consistent with the 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 to include user or screen names, persistent identifiers, identifiers linking children's activity across different websites, the combination of date of birth, gender, and zip codes, or ZIP+4, and photographs, video and audio files, unless linked to some other item of data like a home or e-mail address. Expanding the definition of personal information to data previously deemed anonymous, and applying new limits on important internal uses of information, will create an obligation to collect more information from children and parents to obtain consent, with commensurate new obligations and costs to manage that data. TIA and its members believe that such changes will not provide any added safety benefits to children, will not help to ensure the confidentiality and security of such information, and are wholly unnecessary, particularly when it comes to company websites and families of websites.

VII. DATA RETENTION AND DELETION

A new section proposed by the FTC addresses data retention and deletion. The Commission proposes adding the requirement that personal information be retained only for so long as necessary to fulfill the purpose for which it was collected. This reflects current practice, and TIA agrees that this is an appropriate yet flexible standard that meets business needs. An operator must also delete such information using reasonable measures. The Commission, however, has not fully addressed the burdens imposed by the expanded deletion requirement.

The nature of server systems and data archival efforts makes the complete deletion of any information extremely difficult. A party may be able to delete information from a server, but that server and the deleted information may be backed-up by multiple onsite and offsite servers as well as Cloud services. In actuality, it may take weeks or months before such information is completely removed from a company's records, and it may be a practical impossibility to delete

[24] 76 Fed. Reg. at 59,821 (emphasis added).

it. Any requirements for deletion of personal information should be related to deletion from active marketing databases and tempered with a reasonable efforts standard. In addition, there may be overlap with other laws or regulations that either mandate retention of information for certain periods of time or, conversely, permit longer periods of time for retention of information.

VIII. SAFE HARBOR PROGRAMS

The Commission proposes to impose more oversight on safe harbor programs, requiring such programs to report annually about compliance and to require participants to conduct annual audits. There is limited support in the record for such an expansion. COPPA requires the Commission to offer "incentives" for self-regulation.[25] Imposing added obligations on safe harbor programs and program participants hardly seems consistent with that mandate, and the rationale for doing so is not apparent since these programs have been working well.

IX. COSTS AND BURDENS

The revised COPPA Rule as proposed will reduce user convenience and dramatically increase costs to website operators without necessarily enhancing the privacy of children. The additional processes and procedures mandated under the revised proposed Rule will potentially include privacy policy and operational changes, with related resource-intensive measures, such as organizational management and employee training. In addition to these "soft costs," there will certainly be increased monetary costs with respect to technology acquisition and implementation for companies who will need to purchase additional services and products from vendors. The FTC has not taken these costs into consideration. Furthermore, it will be increasingly difficult to obtain parental consent for these types of mechanisms and may potentially require the collection of more information from or about parents, or force more companies to move to subscription models.

The Commission asserts that the proposed amendments to the COPPA Rule will impose a one-time burden on existing operators to re-design their privacy policies and direct notice procedures and to convert to a more reliable method of parental consent in lieu of e-mail plus.[26] FTC estimates the total burden of complying will be only 60 hours, affecting 2,000 websites. Annualized to 20 hours per year for 3 years, the total estimated burden is 40,000 hours at a cost of $5,240,000. This estimate is based on an assumed labor rate of $150 for lawyers and $36 for technical personnel. These costs are grossly understated. TIA members typically consult with specialized attorneys who understand children's privacy and data security laws. Average rates are 2-3 times the Commission's estimates. Similarly, engaging expert technical personnel can, on average, again involve hourly costs that are 2 -3 times the Commission's estimates.

Further, the estimate does not include costs and burdens of "ensuring" security procedures of third parties, securing deletion, managing parental consents, or updating policies to disclose changes in "operators." In addition, the FTC seems to reference only top level domains and, as such, its estimates for implementation of new verifiable parental consent requirements are very low. Each "website" may have many lower level web pages that will be affected by any

[25] 15 U.S.C. § 6503(b)(1).

[26] 76 Fed. Reg. at 59,827.

changes to the parent site. Depending upon the FTC's final revisions to the COPPA Rule, the time it takes to implement technological changes could more than triple the Commission's 60-hour estimate. To implement changes to a website, resources must be devoted to designing, planning, coding, quality assurance, and testing and must be allocated to ongoing operations and maintenance to ensure smooth operation between and among web pages comprising a website. Consequently, costs are likely to be many multiples of the Commission's estimate.

These estimated cost burdens do not reflect the costs of expanding compliance to technology platforms that were not previously covered by COPPA, including mobile apps, Internet-enabled gaming platforms, VOIP services, geolocation services, premium texting, and coupon texting programs. Many companies will incur new costs of acquisition and implementation of products and services required to comply with the proposed Rule changes as applied to these additional technology platforms. Privacy policies will also have to be revised, as the FTC is essentially erasing common sense distinctions between personal and non-personal information described in most existing TIA members' privacy policies, consistent with the current COPPA rule. To the extent the Commission approves a final rule that eliminates current distinctions between personal and non-personal information, these policies will have to be updated. To the extent this constitutes a "material change" in existing privacy policies, many companies simply do not have a database of parent's contact information to notify them directly of the changes precisely because they have sought to promote anonymity to the maximum extent possible by relying on screen or user names and passwords of child visitors. The possibility that existing databases of children's information will have to be deleted are another enormous cost that the Commission has not attempted to quantify.

Further, the estimated costs do not reflect the ongoing costs of compliance. Ongoing and increased costs required to implement more complex procedures, such as costs associated with age-screening or obtaining and verifying parental consent, have not been accounted for. For example, if the FTC requires a scanned form type of control regime, companies will have to dedicate employees specifically to this task which will require additional salary and benefit costs. These costs, which have not been evaluated by the FTC, should be taken into consideration as should the extra time that parents must spend in utilizing other, more complex methods of consent should the FTC eliminate its e-mail plus method. Periodic updates, not a one-time update, will be needed to accommodate disclosure of new "operators" that reflect changing commercial relationships between the operator and service providers. Finally, the burdens on parents to receive, process and understand those updates have not been quantified. TIA is concerned that parents will be confused about the role of service providers when they receive notices, will be annoyed and angry about getting multiple notices, and will wrongly believe that children's privacy protections have been altered when the changes are an artifact of new, restrictive rules. Thus, companies will have to develop communications tools and respond to complaints from parents who may mistakenly believe that companies are altering data collection practices, another cost that the Commission has not included in its estimate of the compliance burden.

CONCLUSION

The privacy of all our consumers is of central importance to TIA and its members. The COPPA Rule has been effective in protecting children since its inception. 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 full extent of all costs and benefits associated with these proposed revisions must be weighed to avoid any unnecessary and unintended adverse effects on both consumers and on companies that must comply. While there are numerous areas where we believe the Commission's proposal will further these goals, in other areas it falls short. In particular, the unduly expansive definition of personal information, and unduly restrictive definition of support for the internal operations of the website, coupled with the proposed elimination of one of the most useful and well-understood methods of consent, will burden parents and toy company members alike. As a strong advocate for children, and a staunch supporter of consumer privacy, TIA and its members appreciate the opportunity to submit these comments to the FTC in this important proceeding, and looks forward to an ongoing dialogue with the Commission on practical approaches to enhance privacy.

Respectfully Submitted,

Carter Keithley
President

Of Counsel:
Sheila A. Millar
Crystal N. Skelton
Keller and Heckman LLP