**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
1001 G Street N.W., Suite 500 West
Washington, D.C. 20001