1200 G Street NW • Suite 200 • Washington, DC 20005
t. 202.459.0354 • e. info@toyassociation.org

December 9, 2019

Via Electronic Submission: *https://www.regulations.gov*

U.S. Federal Trade Commission
Office of the Secretary
600 Pennsylvania Ave. N.W.
Suite CC-5610 (Annex B)
Washington, D.C. 20580

Re: COPPA Rule Review, 16 C.F.R. Part 312, Project No. P195404

The Toy Association, Inc. (TTA), on behalf of its members, is pleased to submit these comments in response to the U.S. Federal Trade Commission's (FTC or Commission) Request for Comment (RFC) (84 Fed. Reg. 35842, July 25, 2019). By way of background, TTA represents more than 1,100 businesses – toy manufacturers, importers and retailers, as well as toy inventors, designers and testing labs – all involved in bringing safe, fun, and educational toys and games for children to market. The U.S. toy industry contributes an annual positive economic impact of $109.2 billion to the U.S. economy. TTA and its members work with government officials, consumer groups, and industry leaders on ongoing programs to ensure safe play, both online and offline. Our industry supports this timely review of COPPA given technological, market, and other changes with a view to identifying new and better ways to protect the safety and privacy of children. Our members have over 20 years' experience in understanding and implementing COPPA requirements. We appreciate this opportunity to address legal, policy, operational, and practical aspects of the existing COPPA rule and the implications of possible revisions in response to this RFC.

Safety, security and privacy by design are core principles for our members. **We support strong and effective uniform national privacy standards to protect consumers, especially children**. Our industry has championed the goals and objectives of the Children's Online Privacy Protection Act of 1998 (COPPA) (15 U.S.C. §§ 6501–6506) since its enactment. TTA has actively contributed to prior FTC rulemakings to offer practical insights on application of the COPPA Rule and proposed Rule changes. Working with our Children's Online Safety Committee (COSC), TTA has over the years developed a variety of COPPA compliance tools and training materials for its members to assist them in understanding COPPA requirements and implementing them in practice. In fact, before the FTC publicly indicated that COPPA applied to connected toys and other connected children's products, TTA provided compliance guidance to its members advising that child-directed connected toys were subject to COPPA. In 2018, TTA participated in the Consumer Product Safety Commission's (CPSC) Internet of Things (IoT) workshop, and also participated in the recent COPPA workshop held on October 7, 2019.

Notably, toy industry members are affected by a variety of other privacy and data security laws. They include the California Consumer Privacy Act (CCPA) (Cal. Civ. Code § 1798.100 *et seq.*), Nevada SB 220, and California SB 327 (Cal. Civ. Code § 1798.01.04 *et seq.*), as well as the growing set of international laws, including, but not limited to: the EU General Data Protection Regulation (Regulation 2016/679) (GDPR); the EU Electronic Communications Privacy Directive (Directive 2002/58/EC, amended by Directive 2009/136) (sometimes referred to as the Cookies Directive); and related laws and guidance issued by EU authorities, such as the UK ICO Age Appropriate Design code, UK ICO Guidance on the Use of Cookies and Similar Technologies, and French CNIL guidance on cookies and other technologies. **Differing standards impose significant burdens on businesses without resulting in stronger or more effective privacy protections for children and tweens.** Thus, the toy industry is uniquely qualified to comment on the questions the FTC has posted in the RFC.

COPPA has largely withstood the test of time for two principal reasons. First, COPPA created a uniform national framework for children's privacy and a uniform age to identify a "child." Second, COPPA strikes a careful balance between protecting children's privacy, engaging parents, and authorizing legitimate business operations through both COPPA's definitions and exceptions, and by authorizing different means to obtain parental consent depending on the circumstances. This harms-based approach has worked well. Below TTA offers suggestions on how to address some outdated aspects of the COPPA Rule in addition to responses to some specific questions raised by the FTC. We also highlight conflicts between COPPA and other laws.

Executive Summary

These comments begin with a review of the existing COPPA legal framework. Our comments focus on the following issues with a view to identifying areas where COPPA has worked effectively, elements our members believe can be modernized, and issues requiring further discussion:

- Key definitions and implications
- COPPA's online notice and direct notice to parent obligations
- Verifiable parental consent (VPC) methods
- Activities exempt from parental consent
- Parental access and deletion requests
- Confidentiality, security, and integrity requirements
- Safe harbor programs
- Obligations of "operators" providing content on platforms
- Costs and benefits and impacts on small businesses

The list above does not represent a comprehensive list of all potential issues affecting TTA members, but rather identifies those issues most important to TTA in response to the RFC and other developments. These comments also address significant inconsistencies and conflicts with other state, federal, and international laws as we discuss the above points. In this regard, Attachment I, which highlights relevant obligations and inconsistencies, supplements these comments.

To summarize briefly, TTA recommends the following:

- **A risk or harms-based approach to privacy protection, or differential privacy, should continue to be the guiding principle of the FTC's implementation of COPPA as it considers possible updates to the COPPA Rule consistent with statutory mandates.**
- **Congress appropriately identified "children" as individuals under 13 when it enacted COPPA. TTA supports that definition, which aligns with how "children" are defined for product safety and advertising purposes, both of which are of central importance to our industry. However, we believe the FTC can take a leading role in fostering a dialogue about how to enhance tween privacy while allowing for legitimate business activities and a smooth consumer experience.**
- **The FTC should maintain the balance of factors used to determine if a website or online service is directed to children under 1. TTA opposes adoption of numerical or percentage audience thresholds as a determinative factor in identifying a "child-directed" site or service.**
- **General audience sites and services remain crucial to business operations. The FTC should confirm that app stores, sites for adult toy collectors, and e-commerce sites, as well as general use, in-home connected products, are not directed to children.**
- **The statutory actual knowledge standard should be retained.**
- **Sites intended for "mixed audiences" that may include children, tweens, teens, and adults should have the option of age-screening to offer appropriate experiences to different audiences as an alternative to an obligation to treat all visitors as children under 13, but not the obligation to do so.**
- **The FTC must demonstrate that any data element it proposes to list as an item of "personal information" in any revised COPPA Rule permits the physical or online contacting of a child under 13. Inference data does not allow such contact.**
- **It is less clear whether biometric information itself allows the direct physical or online contacting of a child. To the extent the FTC demonstrates that it does, the FTC should also assess the need for exceptions to continue to strike a careful balance of privacy and business needs. For example, collection of biometric information may be necessary and indeed privacy-protective where it is used to enhance the security of a child-directed or other online service.**
- **The support for the internal operations exception in COPPA remains critical to the effective functioning of the internet and the conduct of important business operations and should remain. Based on both the COPPA Rule and Preamble language, TTA believes that advertising attribution is already covered by this exception but supports clarifying this point in any updated Rule.**
- **TTA opposes adding "inference data" to a list of data elements that constitute "personal information" *per se*. Doing so is not only inconsistent with the statutory "actual knowledge" standard, it could undermine the "support for internal operations" exception. An overbroad definition will impede toy companies from effectively and efficiently reaching their core target market: parent purchasers of toys.**

- **The FTC should review COPPA's parental notice obligations in an effort to reduce unnecessary verbiage.**
- **TTA agrees that online services directed to pre-literate children should be assumed to be directed to adults.**
- **Flexibility in allowing a variety of VPC methods tailored to different circumstances remains vital. It is costly to implement robust VPC and doing so results in significant drop-off of interest by parents. More restrictions that force companies to set up pay walls or other parental consent mechanisms will reduce, not foster, children's content online. We urge the FTC to study ways to reduce the "friction" the VPC experience engenders with parents.**
- **We support incorporating into the Rule approaches in FTC guidance that allow schools to obtain VPC on behalf of parents.**
- **The FTC should adopt its enforcement discretion position on managing voice data into the Rule.**
- **The FTC should formalize its position that the parent purchaser of a connected toy is the sole individual who must provide parental consent, if needed, on behalf of all child users.**
- **The FTC should avoid adoption of detailed, prescriptive security requirements in an updated Rule, as they are likely to become outdated quickly.**
- **TTA supports retaining the existing safe harbor framework.**
- **Today's parents use their mobile phones. We urge the FTC to reconsider the option of asking children to furnish a parent's cell phone number as a way of offering notices to parents and initiating VPC where needed.**
- **Much more clarity is needed around the specific obligations of content creators offering YouTube content in the wake of the FTC's recent stipulated order with Google and YouTube. Content creators do not control the privacy notices or practices of the platform, and cannot assume all obligations of "operators" set forth in the COPPA Rule as a result. Additionally, clarity is needed on how such a determination would apply to other platforms, like connected televisions. Importantly, initial guidance from YouTube indicates that content creators must make an "either/or" choice in identifying content as directed to children or not. This simply does not reflect an optimal environment to incentive the production of more family-friendly content. The FTC should consider implications as well on the availability of such content.**
- **In these comments we have identified many instances of inconsistency between various laws and guidance document, both within the U.S. and internationally. Uniformity in applicable legal obligations is critical to safeguarding privacy, facilitating compliance, and reducing compliance burdens, and we identify areas where COPPA preempts inconsistent state law. We also urge the FTC to share its views with other regulators on striking a careful regulatory balance that enhances privacy and facilitates parental oversight, but that allows businesses to manage routine activities and promotes an environment that fosters consumer choice, competition, and innovation.**

The COPPA Legal Framework

Before turning to our specific comments in response to questions posed by the RFC, we first outline the COPPA legal framework. COPPA sets out both a nationally uniform standard and a risk- or harms-based approach to privacy protection that creates a commonsense scheme of differentiated privacy standards rather than a one-size-fits-all approach.

VPC to collect more than limited data from children is a core requirement of COPPA, one that our members agree is necessary and appropriate where potential privacy risks to children are greatest. This occurs, for example, when children's data might be publicly exposed or shared in a manner that allows them to be contacted offline or online. The COPPA framework, however, makes clear that not every data element should be treated identically, that some data collection is essential to business operations or serves a legitimate purpose without unduly affecting the privacy of children or their parents, and that the most robust forms of VPC are neither necessary nor desirable to safeguard children's privacy in each and every instance.

For example, businesses can respond to a child's single email inquiry without obtaining parental consent. Data used to support internal operations can be collected in a manner that does not risk jeopardizing children's privacy or unnecessarily burdens parents, while serving important business purposes. That means businesses can allow a child to sign up with a username or alias and password, hold it in a cookie to allow a child to return to a site without logging in again, and save game scores and activities. Businesses can collect a child's email address for internal company marketing, such as allowing entry into a sweepstakes or promotion or fulfillment of a prize, relying on a less onerous form of VPC, "email plus," to permit the entry and/or award the prize. Businesses can allow a child to send an email to a friend if specific precautionary steps are taken to safeguard privacy. A business can (and indeed must) ask a child to furnish a parent's email address to contact a parent and obtain consent. COPPA recognizes that absent a vehicle to request some type of contact information about a parent from a child, there would be no way to provide notice to parents and start any necessary consent process. Congress and the FTC also wisely rejected the notion that parental consent was always needed before any data that might be defined as "personal information" could be collected. Had Congress and the FTC not created this flexible framework, it would have forced companies to bar child visitors from accessing a website or engaging with an app until some sort of parental consent process had been completed, creating significant barriers for both children and parents without offering meaningful privacy protections.

The FTC recognized in the 2013 COPPA Rule that many data collection activities serve important business functions with no real impact on children's privacy. As the definition of "personal information" expanded to include data elements that at COPPA's inception were not considered "personal," like persistent identifiers, the FTC also clarified that persistent identifiers used solely to support internal company marketing can be collected when it updated the COPPA Rule in 2013. Operators are exempt from parental notice and consent obligations when using persistent identifiers in accordance with the Rule. This crucial exemption allows businesses to not just offer privacy-safe functionality, but also to conduct analytics and utilize data for important business purposes outlined in the Rule and the Rule Preamble. With its differential approach to notice and consent, the COPPA Rule has always reserved the most robust parental consent obligations for instances where information is

publicly disclosed to third parties (*e.g.*, through public postings), or is shared with third parties for that third party's own marketing purposes.

The 2013 Rule update also added a new and extremely useful exception that allows toy industry members to request online contact information from a parent to voluntarily alert them to a child's online activity. 16 C.F.R. § 312.5(c)(2). TTA members strongly supported the addition of this exception, and many members utilize it to help parents stay abreast of their children's online activities. Similarly, many toy companies take steps to moderate and pre-screen information shared by children so that personal information that could allow a child to be contacted physically or online is not publicly disclosed or released, while children can still engage in a social online experience. This is another example of privacy by design in action. Children's privacy is protected without burdening parents with unneeded consent procedures.

Congress expressly created a nationally consistent, commonsense, harms-based approach to protecting children's privacy by including a preemption provision in the law when it enacted COPPA in 1998, stating:

> No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter that is inconsistent with the treatment of those activities or actions under this section.

See 15 U.S.C. §6502(d).

National uniformity is critically important to the toy industry. Apart from COPPA, toy industry members are heavily regulated by an extensive set of preemptive federal product safety laws, including the Consumer Product Safety Act (CPSA) (codified at 15 U.S.C. §§ 2051-2089) and Federal Hazardous Substances Act (FHSA) (15 U.S.C. §§ 1261-1278), as modified by the Consumer Product Safety Improvement Act (CPSIA). Those laws include specific definitions and obligations that affect the toy industry as well as makers of all children's products. For example, CPSIA imposes special obligations on manufacturers of products designed and intended primarily for children 12 and younger. This reference age was intended to align with COPPA. Thus, for both informational and physical product safety purposes – key issues for toy industry members – federal law recognizes that the at-risk population should be defined as under 13. We agree that this reference age should be retained to describe "children."

As noted above, COPPA preempts inconsistent state law. Although the CCPA does not expressly mention COPPA in the list of federal laws that preempt the CCPA at §1798.145, importantly, the CCPA recognizes the preemptive effect of COPPA at §1798.196 of the CCPA, which states:

> This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the California Constitution.

CCPA obligations that are inconsistent with COPPA are thereby preempted, and we identify in these comments many such inconsistencies.

There are also inconsistencies between CCPA rules applicable to tweens 13-16 and COPPA's approach to children under 13 that do not square with the harms-based approach in COPPA or reflect a harms-based policy approach. When Congress enacted COPPA, it deliberately adopted a cut-off age to define "children" based on recognition that tweens and teens have their own developing ambit of privacy and that parental consent models simply will not work. Toy companies largely focus online services to adults and to children, so we do not address here potential legal preemption arguments. However, we do note that the proposed CCPA regulations, and in particular the two-step affirmation process proposed in recently issued regulations, are unlikely to advance tween privacy and will impose significant burdens on businesses who target the ≥13-<16 demographic. Some businesses may elect to adopt age 16 as the age of a "child" in the U.S. even when they do not "sell" personal information, to avoid creating three separate business procedures to manage information: parental consent procedures for services directed to visitors under 13, opt-in procedures for tweens ≥13-<16, and opt-out procedures for those over 16, although requiring 15 year-olds to get parental consent is problematic. **We encourage the FTC to consider action to address tween privacy on a national scale, perhaps by convening stakeholder discussions or a workshop. It is essential that we seek to develop a practical approach that, like COPPA, assesses potential privacy risks against burdens to consumers and businesses**.

Inconsistencies in privacy laws are growing within the U.S., but there is also growing divergence in applicable legal frameworks globally. The EU General Data Protection Regulation (GDPR) was designed to harmonize data protection regulations across the EU. However, there is a lack of internal EU harmonization regarding the age of a "child." The GDPR establishes that where consent is the legal basis of processing and the data subject is under 16, consent must be provided by a parent unless Member States adopt a different age (which can be no lower than age 13). The EU is also considering replacing the E-Privacy Directive with a Regulation. In the meantime, some Member States are working on guidance regarding managing cookies and technologies in light of the GDPR, but guidance from the data protection authorities in the UK and France are not consistent. These differences sow confusion, increase compliance costs, confuse consumers, and complicate the task of bringing to market fun and safe online experiences, without offering any evidence that more restrictive rules result in improved privacy protection for children or tweens.

A hallmark of the toy industry is innovation. Today's large companies typically started with an idea in an inventor's basement or garage. Inconsistencies both within the U.S. and beyond pose special and growing challenges to TTA's many small business members, making strong, uniform, and effective national standards crucial not only to protect consumers, but also to continue to promote a dynamic marketplace of consumer choices for toy products and online services that foster play, education, and entertainment. Given the importance of digital offerings in today's economic environment, the growing divergence of privacy legal standards, within and outside the U.S., poses a substantial risk to a thriving, competitive U.S. and international toy market. Conflicting rules raise costs and pose entry barriers for entrepreneurs with new ideas for toys and related digital offerings. **A risk or harms-based approach to privacy protection, or differential privacy, should continue to be the guiding principle of the FTC's implementation of COPPA as it considers possible updates to the COPPA Rule consistent with statutory mandates.**

TTA Comments

I. Key COPPA Definitions

A. Website or Online Service Directed to Children

The predicate question for any company potentially affected by COPPA is whether it is offering a commercial website or online service targeted to children. 16 U.S.C.§ 6501(10). In this section, we discuss when a service should and should not be considered directed to children, thoughts on possible modifications to the Rule, and inconsistencies between COPPA, the GDPR, and the CCPA in their frameworks and definitions. Inconsistencies start with differing obligations on handling information from "children."

Website or Online Service

COPPA applies to websites, or portions of websites, apps, and connected products "directed" or "targeted" to children under 13. COPPA is limited to the online collection of information from children, whereas other laws, including the GDPR and CCPA, cover online and offline collection. The FTC has identified a variety of factors that can be applied to determine when an online site or service is directed to children. Congress also specified that an operator violates COPPA if it collects information with *actual knowledge* that it is dealing with a child. 15 U.S.C. § 6502(a)(1). A website or online service is not considered to be directed to children solely for referring or linking to a commercial website or online service that is. 15 U.S.C. § 6501(10).

Who Is a "Child" and When is an Online Service Directed to a Child?

When it enacted COPPA, Congress defined a "child" as "an individual under the age of 13," and defined a website or online service subject to COPPA as one "targeted" to a "child" under 13. 15 U.S.C. §6501(1). Congress specifically adopted a reference age of 13 in the statute, recognizing that teens and tweens have their own sphere of privacy and parental consent models will not work effectively with them. The toy industry supports maintaining distinctions between children under 13 and tweens. The reference age of 13 aligns with federal product safety laws and with generally recognized approaches distinguishing advertising to children from advertising to tweens, teens and adults. For example, the Children's Advertising Review Unit (CARU) Self-Regulatory Program for Children's Advertising applies to "national advertising primarily directed to children under 12 years of age in any medium." International bodies, such as the International Chamber of Commerce (ICC) Marketing and Advertising Commission, recognize that advertisers must use special care in advertising to minors, but teens and children should be treated differently because of their differing abilities to understand advertising. *See* ICC Toolkit on Marketing and Advertising to children, available at https://iccwbo.org/content/uploads/sites/3/2017/10/ICC-Toolkit-Marketing-and-Advertising-to-Children-2017.pdf, and ICC Statement of Code Interpretation and Reference Guide on Advertising to Children, available at https://iccwbo.org/content/uploads/sites/3/2017/01/Reference-Guide-on-Advertising-to-Children-Statement-on-Code-Interpretat....pdf. **TTA agrees that age 13 is an appropriate benchmark to define a child for privacy purposes.**

Section 312.2 of the COPPA Rule identifies some key factors to consider in determining whether a website or online service, or portion of a website or online service, is directed to children. TTA largely agrees that these factors have worked well. For COPPA purposes, the content of the website or online service is key. The intent of the creator of the website or online service in identifying the target demographic is another important element in assessing when a site or service is "child-directed." Notably, the COPPA Rule factors also generally align with considerations used to determine when advertising is directed to children or when, for CPSC purposes, a product is primarily designed and intended for children 12 and younger. However, the 2013 Rule change that resulted in a distinction between online services "primarily" directed to children and those that are "secondarily" directed to children has generated some confusion. Industry commonly refers to "mixed audience" sites and online services as those that include children among the target audience.

While the concept of "primarily" directed to children works well where children are the only or predominant target audience, the attempt to distinguish between those sites and sites "secondarily" directed to children has provoked many questions about exactly what this means, especially given FTC guidance indicating that sites directed to children must treat all visitors as children, and only sites "secondarily" directed to children are permitted to age-screen. This question has become increasingly important as rigid distinctions may limit the ability of brands or content creators from reaching multiple audiences in a privacy-appropriate way.

The FTC specifically asks for input on whether there are circumstances where general audience platforms with third-party, "child-directed" content should be able to rebut the presumption that all users interacting with that content are children. The answer is of course they should, but TTA believes this question is too narrowly framed. The majority of many platforms users when considered as a whole are likely to be adults, so the reverse presumption applies. To the extent that a majority of overall visitors to a platform are children, a rigid rule that requires platforms, websites, or other online services with a significant minority of users or visitors over 13 to treat everyone as a child does not best further policy goals of fostering innovation and content while protecting privacy, especially where family-oriented content is concerned. Such an approach fails to recognize the reality of family co-viewing of content. It is particularly misguided where the FTC seeks to encourage platform providers whose platforms are broadly intended for general audiences to take steps to try to respond to potential child visitors. **TTA suggests that the FTC consider revising the Rule to establish that a mixed audience site or service, including apps or platforms, is one that offers content directed to children, but whose target audience likely includes a significant number of tweens, teens or adults**, even if segments other than children do not comprise 50% or more of the audience. In such a circumstance, operators could still elect to treat all visitors as children or implement other appropriate measures to allow all visitors to experience age-appropriate content. This change is especially important to toy companies because online services featuring toy brands and characters both appeal to parents and adult nostalgia fans of our members' brands, and may also target those audiences.

The FTC also asks if online services that attract "large" numbers of child users, even though they do not have child-oriented activities, should be considered to be "child-directed." **TTA opposes adoption of numerical audience thresholds as a single determinative factor to identify child-directed sites or services, whether based on total audiences or percentages.** Doing so is inconsistent with traditional norms for advertising and risks undermining the intent of the statute by elevating a

single factor over others. Such an approach is also entirely inconsistent with how the FTC and advertising self-regulatory bodies handle advertising.

For example, while a large number of children may watch major sports programs such as the World Series, the Super Bowl, or the Olympics, these programs are viewed as intended for general audiences. Advertisers on such programs are not restricted to offering only kid-appropriate ads, and advertising guidelines for child-directed advertising offered by groups such as CARU simply do not apply. While the Rule allows both competent and reliable empirical evidence regarding audience composition, the number of child visitors is simply one factor to consider in determining if a site is child-directed, in whole or in part. It should not be a sole determinative factor. The intent of the operator and whether the actual content is child-directed are more significant and are the factors most in keeping with the statutory definition that only sites or online services "directed" or "targeted" to children, or those with actual knowledge that they are dealing with a child, are subject to COPPA.

These definitions take on special importance where connected products are concerned. Most connected toys are primarily directed to children for COPPA purposes and are indeed "children's products" for CPSC purposes. In contrast, a connected doorbell or refrigerator is a general audience product for both privacy and product safety purposes. It remains vital to retain distinctions between online sites and services available to all and those that are directed to children due to child-oriented content. Historically, the FTC has agreed that many sites children might conceivably visit are general audience sites not subject to COPPA absent actual knowledge that the operator was collecting data from a child.

In 2013, for example, the FTC clarified that in adopting language referring to entities "on whose behalf" information was collected, it never intended the Rule to encompass platforms such as Google Play or the Apple app stores, when such stores merely offer the public access to someone else's child-directed content. 78 Fed. Reg. 3977. There is even less rationale to treat platforms, sites, or services that sell or offer products for adult purchasers to be used by their children as "child-directed." **We therefore urge the FTC to formally recognize that in addition to app stores, sites targeting adult collectors and e-commerce sites that sell toys, games, DVDs, and other children's products are general audience sites.** The operator is not subject to COPPA unless it has actual knowledge that it is collecting personal information from a child under 13 or offers child-directed content itself. Any additional barriers that limit the ability of parents, grandparents, and others adult purchasers from finding information about available toys online and quickly making a purchase will have a serious adverse impact on the toy industry.

At the same time, the FTC should explore ways to encourage app stores and platforms to offer tools to make it easier for parents to manage their preferences, and for app developers and content creators to meet any independent applicable COPPA compliance obligations, recognizing that special challenges apply in the app environment. This point was raised at the FTC's October 7, 2019 workshop.

Consistencies, Inconsistencies and Conflicts Between COPPA and Other Laws

There are differences in scope between COPPA, the GDPR, and CCPA. COPPA applies to data collected through a website or online service directed or targeted to children under 13 or where the operator has actual knowledge that information is being collected from a child under 13. In contrast, the

GDPR and CCPA apply to any type of information collection, online or offline, regardless of the age of the data subject, but establish certain rules about data collected from "children." Neither the GDPR nor CCPA specifically defines a "website or online service directed to children." However, in recent guidance, the UK ICO suggested that an information society service (ISS) "likely to be accessed by a child" had special responsibilities, as discussed below. The "likely to be accessed by a child" standard lacks any cogent guiding principles and conflicts entirely with COPPA's "directed to children" standard. The result might be to treat an ISS as "child-directed" in the UK, whereas such a service could not be considered "child-directed" under COPPA.

The GDPR establishes that data collection must have a lawful basis. Data processing is only lawful under the GDPR if: processing is necessary to perform a contract; processing is necessary for compliance with a legal obligation of the controller; processing is necessary to protect the vital interests of the data subject or another natural person; processing is necessary for the performance of a task carried out in the public interest; processing is necessary for purposes of the legitimate interests of the controller or a third party that are not overridden by the fundamental rights and freedoms of the data subject, in particular where that data subject is a child; or the data subject has given consent.

Where consent is the basis of processing, parents must consent on behalf of a child under the age of consent set by the Member State. Unless a Member State adopts a different age, which can be no lower than age 13, "children" are considered to be those under 16, but EU Member States have in fact adopted various ages between 13 and 16. This approach creates costly complexity and inconsistency within the EU and compliance challenges for businesses. Some companies are implementing age-screens that are geared to the different ages of "children" set by Member States, while others have adopted age 16 as a standard EU-wide. This will result in instances where consumers who have reached the age of consent in a particular Member State are required to get parental permission before accessing certain services but not others. More significantly, as we discuss in greater detail below, post-GDPR guidance from the UK ICO on its laws implementing the e-Privacy Directives indicates that consent will be required to use cookies or other technologies except those strictly necessary to provide the function of the website. This is inconsistent with the "support for internal operations" exception to COPPA, potentially turning many privacy-safe interactions that rely on collection of information from persistent identifiers that qualify under the GDPR legitimate interest basis of processing into interactions that now require parental consent.

The UK ICO has issued a proposed Age Appropriate Design (AAD) code, under which sites "likely to be accessed by a child" should operate when finalized. It is not at all clear what the ICO means by the "likely to be accessed" standard. What is clear is that the draft AAD code will create many inconsistencies with COPPA, starting with an apparent premise that sites should uniformly collect the visitor's date of birth, even if a site or service is entirely directed to children. The code also seems to imply that sites and services must *retain* that information to offer age-appropriate updates and information to the child visitor, or re-screen visitors' ages when new features are added that might affect the types of required age-directed privacy notices. This seems to be inconsistent with concepts of data minimization. COPPA, in contrast, treats all visitors to a site primarily directed to children as "children under 13" and requires sites that are permitted to age-screen to treat under-age visitors as "under 13." COPPA notices, in contrast, are intended for parents. The result may be more geo-fencing, restricting children from more broadly experiencing suitable content internationally because of restrictive regulatory obligations.

The CCPA does not define "children" in the definitions section at §1798.140. Instead, §1798.120(d) prohibits a business with *actual knowledge* that a consumer is under 16 from "selling" for monetary or other valuable consideration personal information of such individual absent consent. Consent must be provided by a parent or guardian for those under 13. Those 13-16 must give opt-in consent using a two-step affirmation process before a business may "sell" personal information. Toy companies typically do not "sell" children's data, and are required to adopt VPC procedures or adhere to exemptions before releasing or disclosing data, including instances where doing so does not constitute a "sale" for CCPA purposes because there was no exchange of monetary or other valuable consideration. Toy companies are not in the business of "selling" children's data but simply want visitors to enjoy their brands and online offerings. But differences between how the CCPA defines a "sale" and COPPA requirements, as well as burdens associated with creating a new opt-in path for tweens, create confusion. Companies may elect to require visitors under 16 to get parental consent, rather than to adopt new opt-in consent measures for tweens. The reason is simple: creating three different business processes to allow users in three different age groups to experience content – one for children under 13, one for tweens up to 16, and one for adults – will likely add too much complexity and cost for many businesses.

B. Personal Information

COPPA allows the Commission to add other "identifiers" to the list of "personal information" if the Commission determines that such identifier permits the physical or online contacting of a specific individual. The revised 2013 COPPA Rule amended the definition of "personal information" in several ways. Among the two most significant were adding a "persistent identifier that can be used to recognize a user over time and across different websites or online services" and a "photograph, video or audio file collected from a child where such file contains a child's image or voice" to the list of "personal information." While serious questions exist as to whether these "identifiers" alone do allow the physical or online contacting of a specific individual, the new data elements were added to the definition in 2013. However, the FTC treated them differently.

For example, information collected using persistent identifiers is not subject to parental notice and consent obligations when the information is used solely to support internal operations. Participants at the FTC's October 7 workshop emphasized the importance of this exception to the legitimate functioning of businesses, given the absence of any material adverse impact on children's privacy. Collecting a photograph, video, or audio file, in contrast, requires VPC, but the FTC staff later issued an important and pragmatic enforcement discretion guidance statement regarding certain specific uses discussed later in these comments. This difference reflects again the underlying premise of COPPA: a flexible and practical harms-based approach to notice and consent is needed. Defining virtually any data element as "personal," and then treating every type of data that might be considered "personal information" identically, fails to advance sound public policy. Doing so unnecessarily restricts important and privacy-safe business operations and inhibits an operator's ability to serve the interests of children and parents without materially enhancing children's privacy. **Adhering to statutory definitions and mandates and fully considering practical implications of decisions to expand the list of "personal information" under COPPA must remain the underpinnings of the FTC's differential privacy approach going forward.**

Consistencies, Inconsistencies, and Conflicts Between COPPA and Other Laws

The GDPR defines the term "personal data" as "any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

While "personal data" is broadly defined under the GDPR, it can be collected and used where it serves a legitimate business purpose that is not outweighed by the fundamental rights of the data subject, in particular, the rights of children. Thus, international businesses can collect certain data from EU children in reliance on this legal basis for processing under the GDPR in a manner that largely aligns with COPPA, including the various exceptions to the parental consent requirement. This approach also allows for flexibility in obtaining parental consent. Indeed, the GDPR approach can provide added flexibility for companies as compared to the COPPA approach in some instances. However, as we note elsewhere in these comments, recent interpretations of the e-Privacy Directive and related Member State laws may restrict important business operations if express affirmative consent obligations are imposed before any "non-essential" technology can be deployed to collect information. In contrast, the exception for data used to "support for internal operations" in COPPA allows businesses to continue to collect data through technology when used solely to support certain business operations. This includes collection of data for analytics, IP protection, contextual advertising, and other purposes, which, while not essential to the basic functioning website or online service, serve important business needs with minimal impact on children's privacy.

There are some definitional similarities between COPPA, the GDPR, and the CCPA, but the CCPA's definitions do not align with COPPA. The CCPA defines "personal information" quite broadly at §1798.140(o)(1). Personal information includes information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The addition of "household" information creates significant potential operational complexities that complicate the task of identifying a "child" under 13 and a "tween" 13 to 16. "Personal information" specifically includes contact details, persistent identifiers, an "alias," characteristics of protected classifications under California or federal law, biometric information, geolocation data, audio, electronic, visual, thermal, olfactory, or similar information; and inferences drawn from any such information. Section 1798.140(o)(2) of the CCPA excludes from the broad definition of "personal information" only "publicly available" information.

Data elements considered "personal" under the CCPA not listed under COPPA, and inclusion of household data, are inconsistent with COPPA. However, the CCPA applies only to the "sale" of personal information of children where the business has actual knowledge the data is from children, so the impact of the requirements is likely to be limited. In fact, since COPPA applies to the "release" of personal information, operators must obtain VPC from parents in many instances where there is no "sale" for monetary or other valuable consideration (for example, where children are permitted to post videos or photographs online), offering broader protections for children under 13 than the CCPA.

C. Support for Internal Operations

As noted above, the definition of "personal information" now includes a "persistent identifier that can be used to recognize a user over time and across different websites or online services." However, the COPPA Rule also defines another term, "support for internal operations," that creates a crucial exception from parental notice, consent, access, and deletion obligations under COPPA. Thus, persistent identifiers can be used for purposes expressly listed in the COPPA Rule as well as for activities described in the 2013 Rule Preamble (78 Fed. Reg. 3,972 at 3,981 (Jan. 17, 2013)). Notably, the "support for internal operations" exception does not cover data collected for online behavioral advertising purposes, which is strictly prohibited under COPPA in child-directed sites or services absent parental consent.

The Commission initially proposed to define the term "support for internal operations" more restrictively (*i.e.*, a "persistent identifier that can be used to recognize a user over time *or* across different websites or online services"). That definition would have effectively barred the collection of data that businesses need to support important legitimate business activities and that allow the internet to function. The FTC ultimately revised the proposed definition in the final Rule, rejecting the notion that parents should always have to receive notice of and consent to the collection of data through technology when it is used solely support legitimate business operations. Being required to do so would have forced companies to block child visitors and obtain parental consent before any type of interaction, preventing them from serving children in a privacy-safe way. The exclusion for actions that support internal operations was and remains crucial to toy company business operations, allowing legitimate business activities to continue in a manner that does not burden parents or infringe children's privacy.

Under the COPPA Rule, IP addresses and other information can be collected and shared to support the internal operations of a website or online service so long as the information collected for such purposes is not used or disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose. 16 C.F.R. §312.2. Under the Rule, support for internal operations means those activities necessary to:

(a) maintain or analyze the functioning of the website or online service;
(b) perform network communications;
(c) authenticate users of, or personalize the content on, the website or online service;
(d) serve contextual advertising on the website or online service or cap the frequency of advertising;
(e) protect the security or integrity of the user, website, or online service;
(f) ensure legal or regulatory compliance; or
(g) fulfill a request of a child as permitted by these guidelines.

When it updated the COPPA Rule in 2013, the FTC specified that support for internal operations also includes activities such as intellectual property protection, payment and delivery functions, spam protection, optimization, statistical reporting, or de-bugging, expressly stating that it did not need to update Rule language for these activities to be covered. *See* 78 Fed. Reg. at 3,980 - 3,981. Allowing an exemption for "advertising attribution" appears consistent with the Preamble language, which characterizes activities like payment and delivery functions, optimization, and statistical reporting to be

covered by the Rule language. Attribution or the ability to trace the source of an action remains important, and COPPA's prohibition on use of persistent identifiers for behavioral advertising serves as a safeguard to assure that use is appropriately limited. TTA would also support adding such an exemption to Rule language if doing so would avoid any confusion on this point.

In short, collection and sharing of information generated by persistent identifiers over time and across websites is essential to provide services and manage business operations. While at the time of the rulemaking many questions were raised about whether any use of persistent identifiers met the statutory criteria for inclusion in COPPA, the uses defined as "support for internal operations" do not allow the physical or online contacting of a specific individual and were properly exempted. **In updating the COPPA Rule in 2013, the FTC recognized that imposing a parental consent obligation where persistent identifiers are used solely to support internal operations would burden businesses and parents without advancing children's privacy, and that attempting to more broadly restrict such use would not be consistent with the statutory language. It is vital that the FTC retain this crucial exemption establishing that persistent identifiers used to support internal operations are not personal information.**

Consistencies, Inconsistencies, and Conflicts Between COPPA and Other Laws

The GDPR and CCPA each take a different approach to the collection of persistent identifiers. The EU landscape is further complicated by the interplay of the GDPR and the so-called "Cookies Directive," as well as a recent court decision and Member State guidance on national law implementing the Cookies Directive. Because businesses have a legitimate interest under the GDPR in processing data used solely to support internal operations (like data used to provide analytics to the business or to allow users to customize certain preferences in a privacy-safe way), parental consent is not needed. This results in general alignment with COPPA and the GDPR. However, a recent decision by the Court of Justice of the European Union and a draft UK ICO interpretation of UK law implementing the e-Privacy Directive could bar the use of technology used to support internal operations under COPPA. That is, the Cookie Directive has now been interpreted to mandate express, opt-in consent for all but "essential" cookies. Essential cookies are those that allow the website or online service to function. This will likely result in differences that could dramatically alter how businesses must structure certain online sites and services. For example, collecting an anonymous username and password and associating it with a cookie arguably is "essential" to allow a child to register at a website to enjoy a privacy-safe anonymous experience. Taking measures to age-screen and using technology to do so likewise seem essential to legal compliance. It is less clear that the full suite of uses permitted under COPPA can continue based on the cookie guidance absent parental consent.

In contrast, under the CCPA, a consumer has the right to request that a business delete *any* "personal information" about the consumer which the business has collected from the consumer (§ 1798.105(a)). The business does not have to actually delete it if it uses the data for specific purposes listed in § 1798.105(d), including a catchall defined as where the business "otherwise use[s] the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information." *See* § 1798.105(d)(9). This limited exception covers only deletion and not access. Because COPPA preempts inconsistent state law, parental consent obligations do not apply where persistent identifiers are collected and used to support internal operations; access and deletion are irrelevant.

Use of persistent identifiers for activities that fall within the category of "support for internal operations" typically do not involve the "sale" of personal information for monetary or other valuable consideration, so would not trigger consent by parents or opt-in consent by tweens. But the anomalous result is that if such actions should fall under the CCPA's broad definition of a "sale" and the conditions imposed on service providers, notice and opt-in consent may be needed for a business to knowingly collect data from tweens ≥13-<16 to support internal operations. Similarly, access and deletion requests related to data used to support internal operations are irrelevant where the information involves children under 13 because of the COPPA exemption, but may trigger access requests for tweens. It is hard to see how an approach that departs so significantly from COPPA provides meaningful privacy benefits.

D. Inference Data

The FTC also asks whether information that is inferred about, but not directly collected from, children should be specifically included in the list of "personal information." First, inference data does not permit the physical or online contacting of a child. Even if it did, the concept of treating inference data as personal information is puzzling since a fundamental premise of COPPA is the assumption or "inference" that visitors or users of a site or online service primarily directed to children are, in fact, all children under 13. General audience sites are subject to COPPA only if they have actual knowledge that they have collected personal information from a child. If a general audience or mixed audience sites age screens visitors, individuals screened as under age 13 are all presumed to be children under 13 and are either blocked from accessing the service or offered age-appropriate content.

The COPPA Rule circumscribes the scope of the internal operations exception by establishing that the data cannot be used to contact a specific individual, including through behavioral advertising or to amass a profile on a specific individual. The exception does allow standard use of persistent identifiers to offer some types of privacy-safe personalization – for example, linking a user name and password to an IP address or other device identifier, allowing children to save game scores and activities, and to recognize returning visitors – and are permitted within the support for internal operations exception. Likewise, collection of analytics data used to support contextual advertising, fraud, and IP protection and other activities is permitted under COPPA. Data collected to support internal operations at a child-directed online service of course "infers" that the data may be linked to a child, largely as an artifact of the FTC's determination that child-directed services must treat all visitors as children, but those inferences are innocuous. A more restrictive approach would have the perverse effect of forcing operators to get parental consent, requiring the collection of additional information in lieu of the limited data collection involved to support internal operations. This would be contrary to the concept of data minimization that underlies COPPA.

Parents, grandparents, and others who seek to purchase toys for the children in their lives typically search online for information about toy options. Often adults who are "nostalgia fans" of the toys and games they remember from their own childhood gravitate to purchasing some of the same toys they loved as children themselves. They might be categorized as a "[toy brand] lover," or as a "toy car" or "doll" lover based on that behavior, but no inference can be drawn about the age of anyone operating the device by characterizing the individual as such. COPPA permits the FTC to add new items of data to the list of "personal information" to the extent that data allows the online or offline contacting of a child. Inference data does not allow the online or offline contacting of a child and thus does not qualify for listing. **TTA opposes adding "inference data" to a list of data elements that constitute "personal information" *per se*. Doing so is not only inconsistent with the statutory "actual knowledge"**

standard, it could undermine the "support for internal operations" exception. An overbroad definition will likewise impede toy companies from effectively and efficiently using targeted advertising to reach their core target market: parent purchasers of toys.

Consistencies, Inconsistencies and Conflicts Between COPPA and Other Laws

The GDPR broadly defines personal data as information relating to an identified or identifiable natural person. To the extent inference data might be covered under the GDPR, however, its use in circumstances covered by COPPA's support for internal operations exception is generally permitted under the legitimate interest legal basis of processing (although, as indicated earlier, this use could be restricted based on some Member State's interpretations of how cookies may be used.)

We have addressed above inconsistencies with the CCPA which specifically added "inference data" to the list of personal information. Inference data is not and could not be considered "personal information" under COPPA. Inference data, like "toy lover" or "[toy brand] lover," does not establish that a business either has actual knowledge that it is "selling" personal information of someone under 16 or is willfully disregarding that information.

E. Other Types of Information

The 2013 Rule identifies as personal information a photograph, video, or audio file collected from a child where such file contains a child's image or voice. In this regard, the FTC issued an enforcement policy statement on October 20, 2017 indicating that it will exercise enforcement discretion regarding handling voice recordings of children provided that the recordings are carefully handled. TTA and its members support this commonsense approach, which is particularly important for certain connected toys. **We urge the FTC to formalize its voice data enforcement guidance as an exclusion in the Rule.** Voice activation is growing in importance as a tool to assist individuals, including children, who have hearing impairments. Voice recordings are typically used to support speech recognition services, which are not necessarily biometric markers of a specific individual. While industry did not challenge the addition of photographs, videos, or audio files to the list of personal information when COPPA was amended in 2013, these data elements, without more, do not allow the direct physical or online contacting of a child.

The RFC asks whether other types of data, such as genetic data, retinal patterns, or biometric data, should be expressly added to the list of "personal information" subject to COPPA. It is not clear that these types of biometric data allow the physical or online contacting of a child without combining it with additional information. In any event, additional types of biometric data, like retinal scans and fingerprints, are not likely to be collected by toy companies. It is worth noting, however, that more device manufacturers are adopting facial recognition and fingerprint scans as enhanced security measures to authorize and validate access to the device. **To the extent the FTC proposes to add new biometric data elements to the definition of "personal information," we urge that it continue to adhere to the statutory language and to also strike a careful balance between reasonable collection needed to support specific uses and business needs, including increasing security measures in the interest of protecting consumer privacy.** If the FTC can establish that these biometric data are personal information subject to COPPA, it may need to consider an exception for collection used to enhance security.

II. Notices to Parents

COPPA mandates that notices be provided to parents, including a notice at the website or online service and via direct notices in appropriate circumstances. Notice and consent obligations do not apply to the collection of data through persistent identifiers so long as the data is used solely to support internal operations. 78 Fed. Reg. at 3980. The Rule requires that notices contain specific information, and the 2013 Rule revisions resulted in mandating separate direct notices to parents depending on the circumstances. 16 C.F.R. § 312.4(c). We urge the FTC to eliminate unnecessary verbiage from the existing mandated notices. Micromanaging notice obligations forces companies to lengthen notices.

In response to questions about how to deal with pre-literate children, **TTA agrees that online services directed to pre-literate children should be assumed to be directed to adults.** For example, it is absurd to think that a connected baby monitor is directed to anyone other than a parent. These products, which often feature a camera and microphone, are, of course, set up by a parent. Baby monitors that operate remotely are not considered "children's products" for purposes of product safety rules, since they are not intended to be "used" by the child. Where entertaining content is intended for pre-literate children to view and enjoy, such as apps for pre-schoolers, the business is entitled to assume that the parent is involved.

Consistencies, Inconsistencies and Conflicts Between COPPA and Other Laws

GDPR Article 5 sets forth principles relating to processing of personal data, including that data be processed lawfully, fairly, and in a transparent manner in relation of the data subject. Proposals to implement the GDPR have shown greater divergence, partly because of the notion that the "data subject" has the rights created under the GDPR and because of how the "Cookies Directive" and implementing national legislation are being interpreted. The UK ICO, for example, suggests that companies offer multiple different types of notices to children explaining their privacy practices, like cartoons or videos for very young children that make privacy understandable. Yet the COPPA framework is designed to put parents in control, requiring that businesses provide notice to parents on their websites or services, as well as, in some circumstances, direct notice to parents, rather than to children. Further, the interplay of the draft UK Age Appropriate Design code and the draft UK ICO cookie guidance require explaining in child-friendly language concepts like analytics derived from persistent identifiers to children who are not being asked to share personal contact details, such as their name and address. Contact details represent a category of "personal information" that is much more understandable to a child then the amorphous concept of persistent identifiers, yet many toy companies never collect contact details from a child. Finally, as noted earlier, we are concerned about the implication that a site or service that the UK ICO might deem is "likely to be accessed" by a broad age range of children will not only have to provide multiple different notices, but either retain birthdate information to provide updated information on new features in the recommended "age-appropriate" format or re-screen children, even if fundamental data collection practices have not changed. This may force companies to restrict access through geo-fencing or other measures.

Notably, the CCPA proposed regulations outline 18 specific items or practices that must be disclosed in a CCPA privacy policy (some of which appear to be duplicative). Some of those, like the obligation to state whether or not the business sells the personal information of minors under 16 without authorization, are puzzling, as doing so is not permitted by the CCPA. The tension between admonitions

regarding user-friendly privacy policy and proscriptive, specific disclosure obligations is evident in these requirements.

III. Verifiable Parental Consent

The FTC has consistently recognized that flexibility is needed to balance privacy rights of children, and the interests of parents in controlling how their children's data is collected and used, with legitimate business needs and operational simplicity to avoid undue burdens on them all. COPPA recognizes a variety of important exceptions that obviate the need to obtain parental consent at all where potential risks to children's privacy are low and burdens are high. For example, operators may collect a child's email address to respond to a one-time message from a child. While not reflected in Rule language, the FTC has also long recognized that a business can collect an email address from a child's friend to send a one-time message to the friend, so long as the email addresses of the child and the friend are promptly deleted, the e-card or message does not contain open text boxes, and the operator, not the friend, sends the message. This position is reflected in the FTC's COPPA FAQs, and would be another candidate for an express exemption in the Rule. Notice and consent are not needed to collect persistent identifiers solely to support internal operations. All of these commonsense exclusions and interpretations minimize burdens on parents and businesses alike.

The FTC has also recognized that where parental notice and consent are needed, different parental consent mechanisms should apply in varying circumstances, reflecting approaches reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. When the COPPA Rule was first finalized in 1999 (64 Fed. Reg. 59888, November 3, 1999), the FTC determined that "email plus" should be approved temporarily in instances where certain information was needed to support internal marketing, like collecting a home address to award a prize in a sweepstakes or contest. The FTC did so hoping to "incentivize" alternatives that might be more robust. Over the years, it became clear that email plus was a reasonable and cost-effective way to obtain consent in instances where data was used solely for internal marketing purposes. The email plus method of consent for internal marketing uses was therefore made permanent in 2013.

In contrast, robust VPC obligations are reserved for situations where children's personal information is disclosed to a third party for purposes that go beyond the support for internal operations exception (*e.g.*, for use in interest-based advertising) or where the child's personal information is publicly available. Authorized methods include use of a credit card with a transaction, a signed consent form, manned toll-free numbers or video services, or newer methods such as using infomediary services to collect information, like a parent's Social Security number. The FTC also provides a mechanism to recognize new forms of VPC. It remains important for the COPPA Rule to establish a procedure to recognize new forms of VPC while allowing operators the flexibility to choose among various methods that work best for them where robust VPC is needed.

The FTC also recognized the importance of creating a mechanism for schools to consent on behalf of parents in instances where schools are using educational technology, saying:

> … where an operator is authorized by a school to collect personal information from children, after providing notice to the school of the operator's collection, use, and disclosure practices, the operator can presume that the school's authorization is based on the school's having obtained the parent's consent.

64 Fed. Reg. at 59903.

The FTC provides further guidance on the use of connected technology in schools in its FAQs and guidance on parental consent. **This guidance is not only useful for school situations but reflects practical limitations of mechanisms for parental consent in various situations outside school settings, and should be embodied in Rule language.** With the growth of connected products, it is not possible for an "operator" to obtain VPC in each situation where a connected product directed to children is concerned. Toys are made to be played with, so whether the connected toy is too large to take from the home or is portable, data might be collected from other children, either inside the parent's home or elsewhere. The operator has no way to identify children from the same family, friends that visit the home, or friends that the child visits with the connected toy. If consent is needed, it can be provided only by the adult purchaser of the connected children's product. **TTA urges the FTC to formally recognize that parental consent by the parent who purchased a connected children's product fully satisfies the operator's COPPA obligations.** It is impractical to take an alternative position, and doing so could result in the elimination of safe, fun children's connected products, including many that fall in the STEM and STEAM categories.

In short, the toy industry agrees that more robust VPC methods are relevant where potential risks of disclosing personal information of children are higher, since the enumerated VPC methods are costly and burdensome to parents and businesses alike. This can lead to frustration, poor consumer experiences, and a significant drop-off in interest. **We favor further discussions about VPC, perhaps through convening a meeting of stakeholders or another workshop, to explore measures to reduce the costs and burdens of VPC methods.** We also encourage exploration of a possible role for the major app stores.

Consistencies, Inconsistencies and Conflicts Between COPPA and Other Laws

To date, the EU has not provided much guidance on specific methods for parental consent. Businesses operating in the EU typically have used the parental consent methods identified in the COPPA Rule in similar circumstances.

The proposed regulations implementing the CCPA outline specific methods for obtaining parental consent to the collection of information from children under 13 and impose an obligation to "establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child." While the listed methods in proposed § 999.330 generally track COPPA's approved methods for scenarios requiring robust VPC, the proposal makes no mention of the sliding scale approach reflected in COPPA and the COPPA Rule, nor does it account for any exceptions, although this is not a significant conflict because the email plus method of VPC does not involve a "sale." However, COPPA imposes a parental consent obligation in a variety of instances that do not involve a "sale" which are not covered by the CCPA. For if example, a child-directed site simply allows children under 13 to post videos, pictures, or other content so it is accessible to third parties, CCPA would not require parental consent at all, even if the business had actual knowledge that it was dealing with a consumer under 13, and would not require opt-n consent by a tween, because no "sale" of the information occurred. In this scenario, while there is no exchange of consideration, robust VPC would be required under COPPA on child-directed sites or services. CCPA proposed rules also impose a documentation obligation. While

COPPA does not impose a specific obligation to document the process adopted, as a practical matter, an operator would have to identify and explain the VPC method used in response to an enforcement action.

Notably, the draft CCPA regulations impose an obligation to obtain "affirmative authorization" before collecting or maintaining any personal information from consumers 13-15 that it intends to "sell." The broad definition raises practical considerations. For example, suppose that an online service allows a 13- to 15-year-old to enter a sweepstakes by voluntarily filling out a form, and asks if the registrant would like to receive offers and updates from the company furnishing the prize. This could constitute a "sale" under the CCPA. Section 1798.140(t)(2)(A) of the CCPA creates an exception for instances where a consumer uses or directs the business to intentionally disclose the PI or uses the business to intentionally interact with the third party, but the inartful wording of the statutory language creates questions about whether this exemption applies where tweens are concerned. If this exception does not apply, the draft regulations require that the business must "clearly request" an "opt-in" for "selling" the information and then also ask the tween to "separately confirm their choice to opt-in." The act of filling out a form and checking a box should adequately serve as the affirmative authorization to use the email for the purpose specified and to share it with a third party.

IV. Right of Parent to Review Personal Information Provided by a Child

Under § 312.6 of COPPA, a parent whose child has provided personal information to a website or online service under COPPA may, upon request, obtain a description of the specific types of personal information collected from children, can refuse to permit further use or collection, direct deletion, and may review any personal information collected from a child. The operator must ensure the requestor is a parent, taking into account available technology, and the mechanism used cannot be unduly burdensome to the parent. The operator is not responsible for good faith disclosures made in accordance with reasonable procedures and may terminate any service where a parent has refused to permit the further use or collection or directed the operator to delete the child's personal information. As a practical matter, because COPPA's notice obligations require disclosure of types or categories of data collected, and because child-directed websites seek to adhere to data minimization principles, members of the toy industry have received relatively few requests to access or delete children's personal information over the years. Although the FTC did not specifically request comments on this obligation, we highlight important conflicts with this provision of COPPA and the CCPA in particular. **TTA opposes adding more requirements to existing procedures for parental access and deletion requests.**

Consistencies, Inconsistencies and Conflicts Between COPPA and Other Laws

The recently issued proposed CCPA rules set forth proscriptive requirements for businesses to receive and respond to access and deletion requests. A business must provide two or more methods for submitting requests (three if the business primarily interacts with customers in person at a retail location). § 999.312. These methods include at a minimum a toll-free number and a website if the business operates a website or mobile app; businesses may also allow requests to be submitted via email, via an in-person form or a mail-in form. We believe that these obligations conflict with COPPA. As noted earlier, definitions of "personal information" are not consistent; operators are not obligated to provide access to or delete information that isn't "personal information" under COPPA.

Requests to access and delete children's information under COPPA must be submitted by the parent, and the operator must take steps to verify that the requestor is actually the parent. The parental

authorization process at § 999.330 does require reasonable steps to determine that the person authorizing a "sale" of personal information is the parent, but this process is at odds with the provisions at § 999.326 which allow an authorized agent to make access or deletion requests. COPPA requires businesses to avoid undue burdens to parents; the two-step process for deletion requests conflicts with this mandate. CCPA deletion requests require a two-step process.

COPPA makes no provision for an "authorized agent" to submit access or deletion requests, another area where CCPA is in conflict with COPPA's requirements that operators take reasonable steps to confirm that a requestor is indeed a parent before disclosing any information collected from a child.

V. Reasonable Security

COPPA imposes a general obligation that businesses "[e]stablish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children." 16 C.F.R. § 312.3(e). The toy industry strongly supports implementation of reasonable and effective security measures to safeguard children's privacy. The FTC has provided a variety of helpful general business guides on security measures, and other federal resources are available as well. For example, the National Institute for Standards and Technology (NIST) has issued a management framework for security that provides a flexible, process management-oriented approach.

Because security threats change so quickly, mitigation strategies must also be adaptable. From that standpoint, it seems inadvisable to enshrine in COPPA Rule language specific requirements for security. Effective security starts with the data minimization principle at the core of COPPA; operators should collect only the information they need to offer the online service and to effectively manage their business. **Specific, detailed security obligations embodied in Rule language could, in a relatively short time, be outdated and thus risk exposing the data that companies seek to protect. We urge the FTC to avoid such action.** This is an area where education and awareness are key. The FTC could collaborate with agencies such as the NIST to increase awareness of their privacy and security resources.

Consistencies, Inconsistencies and Conflicts Between COPPA and Other Laws

COPPA, the GDPR, and the CCPA do appear to establish a consistent general framework that security must be reasonable and risk-based, without adding specific details. The growth of connected products has generated legislative responses such as California's SB 327. While much of the law is appropriately general in nature, SB 327 includes a specific obligation in relation to default passwords. COPPA does not include a similar obligation, but password security is considered a best practice. **Detailed, prescriptive security requirements embodied in statutory or Rule language should be avoided. Fragmented security measures will create confusion and risk becoming outdated. This adds to costs without creating incentives for businesses to invest in management systems and enterprise security approaches.** The perverse potential result might be less, not more, security, as businesses expend resources to deal with a multiplicity of standards.

VI. Safe Harbors

When it enacted COPPA, Congress established a framework to incentivize self-regulation by providing a mechanism to recognize safe harbor organizations. 16 U.S.C. §6503. CARU was the first recognized COPPA safe harbor program. Several other COPPA safe harbor programs currently exist,

including the Electronic Software Ratings Board (ESRB), which also operates a program to rate the content of games and apps. To be recognized, a safe harbor organization must submit a detailed proposal to the FTC, and changes to the safe harbor organization's procedures must likewise be approved. Complaints involving members of safe harbor organizations recognized by the FTC are generally referred to the safe harbor organization. Safe harbor programs can help educate participants, assist in audits and review of privacy practices, and allow the FTC to devote resources to higher priorities. One key value of any safe harbor program is that it creates an environment where participants are encouraged to candidly share plans and operations with the safe harbor organization, and where potential violations of COPPA can then be quickly identified and corrected. Changes to the safe harbor program under which possible violations and the company involved must be publicly identified are likely to be counterproductive and decrease, rather than increase, interest in joining a safe harbor program. **TTA opposes changing the existing safe harbor framework in ways that might eliminate incentives to participate or for participants to candidly share operational and technical issues about COPPA compliance with the safe harbor organization.**

Even when an operator does not formally participate in a COPPA safe harbor program, the FTC has taken action in response to referrals from CARU, including, most recently, the case involving TikTok, which resulted in a civil penalty of $5.7 million. Self-regulatory actions in the children's space have been particularly helpful over the years. Importantly, prior to enactment of COPPA, CARU adopted children's privacy provisions in its advertising guidelines. The framework set out in the CARU Guidelines helped form the underpinnings of COPPA, and COPPA formally recognizes a role for safe harbor organizations. Any changes to the safe harbor program should be carefully calibrated to encourage participation as a route to compliance, as this will best serve the interests of protecting children's privacy and promoting broader compliance.

VII. Other Issues

A. Clarifying Obligations of Platforms and Content Creators

The recent announcement of a stipulated order between the FTC and Google relative to YouTube has complicated the tasks of identifying when and if a website or online service is directed to children, and who is an "operator" for purposes of the various obligations of COPPA. *Federal Trade Commission and People of the State of New York v. Google LLC and YouTube, LLC,* Case No.: 1:19-cv-02642, Proposed Stipulated Order for Permanent Injunction and Civil Penalty Judgment, released September 4, 2019. In the 2013 Rule, the FTC identified YouTube as a general audience platform for purposes of its amendment governing photos, videos, and audios, stating that "this amendment would not apply to uploading photos or videos on general audience sites such as Facebook or YouTube absent actual knowledge that the person uploading such files is a child." *See* 78 Fed. Reg. 3972 at 3982 (January 17, 2013). Changing patterns of use have affected the YouTube audience mix over the years. The toy industry appreciates the FTC's efforts to address market changes that affect COPPA obligations. However, the implications of this decision are far-reaching, affecting not just YouTube, but other platforms, apps, and connected products as well. This RFC offers an important avenue to begin the process of updating the COPPA Rule as to how it applies to content creators and to third parties engaged in behavioral advertising in a manner that fully complies with the Administrative Procedures Act (APA).

FTC Chairman Simon's prepared remarks announcing the FTC's agreement with Google and You Tube emphasized that YouTube had *actual knowledge* that content creators in some instances uploaded child-directed content, but stated:

> For those who create child-directed content to upload on YouTube, the message from today's case is that the FTC considers these individual videos and channels to be "websites or online services directed to children" under COPPA. Once the order has been effective for a period of time, the Commission will conduct a sweep of the YouTube platform to determine whether child-directed content is being properly designated, to ensure that channels are complying with COPPA.

Prepared remarks of Chairman Joe Simons at YouTube Settlement Press Conference, September 4, 2019, available here.

Application of the actual knowledge standard in the YouTube Order is consistent with statements by the FTC in the Preamble to the 2013 Rule that YouTube is a "general audience" platform subject only to the actual knowledge standard, but is inconsistent with Preamble guidance establishing that the actual knowledge standard applied *only when the individual uploading the video is a child*. *Id.*

While industry appreciates the advance notice of a future "sweep" through the Chairman's prepared remarks, broad statements that content creators on YouTube are "operators" subject to COPPA raise significant practical questions. It appears that the goal of the proposed stipulated order is to establish a system where content creators "flag" content as child-directed so that the platform can work with them to assure that children's privacy is protected, rather than to take the position that content creators have an independent obligation to comply with every element of the COPPA Rule. Content creators on third-party platforms are simply not in a position to control many business practices and operations that are implicated by characterizing them as "operators" under the Rule, but that is not sufficiently clear.

For example, how would content creators comply with all elements of the COPPA Rule, such as the obligation at 16 C.F.R. §312.4 to post privacy notices that list all "operators" collecting information at the site, send direct notices to parents, or be responsible for platform security? With potentially thousands of channels on YouTube, including many that might be "child-directed" or mixed audience, does the FTC expect YouTube to list each individual YouTube channel in its privacy notice? Do content creators simply have to cooperate with YouTube in identifying whether content is "child-directed" to have fulfilled their asserted COPPA obligations as contemplated by the stipulated order? If a business advises YouTube that certain content is child-directed, but YouTube fails to honor the designation, is the content creator nevertheless strictly liable under COPPA? Because many toy businesses use these platforms to target adult nostalgia fans, what options do they have to continue to use these important platforms to target adults?

Chairman Simon's prepared remarks suggest that content creators must decide whether content uploaded to YouTube is child-directed or not, suggesting that this is a binary choice. The stipulated order does not discuss a process for content creators to identify mixed audience sites in a manner already permitted by the Rule. Based on the initial guidance offered by YouTube, however, no such option is available. Content creators indeed must provide a simple "yes/no" response in terms of whether content

is "child-directed," when the reality is much more complicated. To the extent YouTube (or another affected platform) is foreclosed from, or fails to offer, a mechanism to address mixed audience content, content creators will potentially be prevented from reaching important audiences via the platform. Again, content creators do not control YouTube (or any other platform), so have no ability to implement an age-screen or other technical measures to restrict access by underage children while allowing those over 13 to access content suitable for them. Only the platform can make that option available.

The FTC's RFC asks whether platforms should have the ability to "rebut" a presumption that it is child-directed. This question seems at odds with the notion that platforms themselves are independent "operators" for COPPA purposes. Of course, the factors in the COPPA Rule must be applied to the specific facts and circumstances involved to determine whether the platform in its entirety is child-directed. The fact that some, or even many, channels on a platform include child-directed content does not mean that the platform itself is child-directed. Television channels may offer a mix of content to a variety of audiences; the fact that some may be directed to children doesn't mean that the entirety of the channel is. Again, however, the way the FTC poses the question suggests that platforms and content creators must make a binary choice, which is not consistent with COPPA.

In short, declaring that YouTube content creators are COPPA "operators" represents a substantial change that triggers questions about which of the specific compliance obligations applicable to "operators" under the current COPPA Rule will apply. As noted above, content creators simply cannot comply with all elements of the COPPA Rule that apply to "operators," and as a result have no real understanding of how to put in place businesses processes to comply.

The Chairman's remarks also have implications for other social media platforms and channels on interactive or streaming television platforms. Much more thought needs to be given to how the suite of COPPA responsibilities might apply in this complex environment. **The FTC must assure that it continues to distinguish between general audience platforms and those directed to children, and must address which specific obligations apply to platform owners versus content creators after a full notice and comment rulemaking proceeding. Likewise, the FTC should further assess approaches to mixed audience content.**

B. Connected Products

Any change in the definition of an "operator" also has significant implications for connected devices. A connected toy is typically directed to children, and operators must take steps to assure that the information collected via the device and a companion app complies with COPPA. However, many apps for children are operating through connected home hubs. The physical home connected hub is not directed to children, but what obligations apply to connected hub operators and to apps and others who offer apps or services directed to children through a home hub? The YouTube settlement agreement therefore seems to have implications for those products as well, which again require significant thought. It remains important to preserve distinctions between connected products that are directed to children and those that are not. Characterizing a product like a home hub as "child-directed" for privacy purposes could be inconsistent with and therefore implicate physical product safety obligations.

C. Costs, Burdens and Impact on Small Businesses

The majority of TTA's more than 1,100 members are small businesses. Regulatory changes have a significant impact on small businesses. Historically, the FTC has substantially underestimated the cost of changes to the COPPA Rule; companies expended considerable resources to update internal procedures when the Rule was updated in 2013. TTA members report that they typically hire technical, consulting, and legal experts to assist in their compliance efforts. Some companies participate in safe harbors. Some offer portals for parents or establish parent accounts. Many members use external experts or tools to conduct privacy and security scans and penetration tests of apps, websites and connected products, and the like of toy websites, apps and connected toys. Toy companies also typically consult with experienced and sophisticated outside privacy counsel to assist them on complicated COPPA questions. Toy companies report that the average hourly rate of the type of experienced external privacy counsel can range from approximately $500 to over $850 an hour.

Some TTA members outsource VPC procedures by using third-party vendors, which involves set-up fees plus per-record costs, and software as a service (SAAS) or other agreements. Based on information provided at the COPPA workshop, the cost of obtaining VPC to collect voice data, photos videos or other content from children, including for public posting online, can average $.35 per record, which leads to considerable drop-off in interest and can be characterized as an unrecoverable lost opportunity cost. Similarly, while members typically report receiving very few requests from parents to access and delete or update children's information (which they largely attribute to good data minimization practices), they incur fees to make those procedures and mechanisms available to parents.

Total COPPA compliance fees for toy companies currently depend on the amount and types of websites, apps and other online services that they offer. External COPPA compliance costs for large toy companies with complex systems and many properties can approach the $2 million range. The above estimates cover external costs only, and do not include the time that in-house toy company engineering, technical, legal, security, marketing and other personnel devote to COPPA compliance obligations. Similarly, this estimate does not include time from in-house personnel to review, strip and screen postings from children to delete any personal information where that function is housed internally. Costs to comply with the plethora of other privacy laws that toy companies are subject to are likewise over and above this estimated total.

Anticipated costs and burdens of a revised COPPA Rule on toy companies are impossible to estimate until draft Rule language is available, but they will almost certainly exceed current costs, possibly by a considerable amount. In particular, changes in definitions of "operators" and in the factors considered to determine if a website or online service is directed to children will dramatically affect costs and burdens. Even if COPPA Rule changes are minor, children's privacy is a highly specialized area where support from seasoned practitioners is needed. Expanded definitions that alter the scope of application of COPPA could significantly increase compliance costs, potentially reduce advertising effectiveness, and restrict the ability of toy companies to engage with parents and caregivers, who are the primary purchasers of toys.

Conclusion

Protecting the privacy and security of consumer data, especially data obtained from children, is central to building consumer trust for toy companies. The toy industry supports strong national consumer privacy and safety frameworks that create a national uniform approach. It appears that tweaks to the Rule, not wholesale changes, would benefit parents, children, and businesses alike. Uncertainty remains, however, about how to treat data collected from tweens. While we support measures to offer younger tweens more privacy protection, the CCPA approach is both unwieldy and unwise, as it does not reflect the concept of differentiated privacy central to COPPA. We urge the FTC to share with the California Attorney General background on how the Commission balanced policy goals when it updated the COPPA Rule in 2013 so that operators can continue to make available privacy-safe sign-ups for children and tweens, administer sweepstakes and promotions using the email-plus method of consent, and engage in permitted analytics and other important business activities without triggering unneeded parental or individual notice and consent obligations. Likewise, the FTC should explore ways to share its considerable expertise with other governments to advance common privacy and security goals in a manner that also accommodates business requirements and a robust competitive landscape. Any proposed changes will be subject to notice and comment rulemaking, but as with prior reviews, changes must be justified based on demonstrating that they will enhance children's privacy while fostering innovation, assure a smooth consumer experience, and include a thorough evaluation of the costs and benefits.

We hope these comments will assist the FTC as it reviews the many important issues posed by the RFC. Please contact Ed Desmond at edesmond@toyassociation.org or Leigh Moyers at lmoyers@toyassociation.org if you would like additional information on our industry's perspective.

Sincerely,

Steve Pasierb
President & CEO

Enclosure

cc: Sheila A. Millar, Of Counsel

ATTACHMENT 1
Comments of The Toy Association
COPPA Rule Review, 16 C.F.R. Part 312, Project No. P195404
INCONSISTENCIES/CONFLICTS BETWEEN COPPA AND OTHER LAWS

Requirement	COPPA	GDPR	CCPA	Observations
Scope	Commercial website or online service doing business in interstate commerce.	Any enterprise that offers goods or services to or monitors the behavior of individuals in the EU.	Commercial enterprise doing business in California that either: • Has >$25 million in revenues, • Buys, sells, receives, sells or shares for commercial purposes PI of 50,000 or more consumers, households or devices, or • Derives 50%+ annual revenues from selling consumer PI	GDPR applies to all enterprises. Non-profit organizations are not subject to COPPA or the CCPA.
Preemption	COPPA preempts inconsistent state law.	The GDPR applies to all Member States without the need for implementing national legislation, except that Member States may set the age of a "child" no lower than 13 and no higher than 16. The related E-Privacy Directive has been transposed into Member State Law.	Preempts certain named state and federal laws, and also specifies that the CCPA "shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution."	Requirements for obtaining affirmative authorization from parents for sale of information of children under the age of 13 in the proposed CCPA regulations are stated to be "in addition" to any parental consent requirements under COPPA. However, COPPA preempts inconsistent laws.
Website or online service directed to children	A website or online service (or portion thereof) that is directed (targeted) to "children," further defined as an individual < 13. Additionally, online services that have actual knowledge that they are dealing with a child are also covered. Only	Not defined; all data is covered. Special rules apply to information collected from "children" (< 16 or as defined in Member State law, which may not adopt an age below age 13).	Not defined; all data is covered. Special rules apply to individuals < 16.	U.S. product safety law defines a "children's product" as a product "designed and intended primarily for children 12 and younger." The Children's Advertising Review Unit (CARU) considers "children's advertising" to be "national advertising

Requirement	COPPA	GDPR	CCPA	Observations
	data collected online from children < 13 are covered.			primarily directed to children under 12 years of age. The draft UK ICO Age Appropriate Design Code proposes to impose obligations apply on all information society services "likely to be accessed by children in the UK." This is a very different standard than the "primarily directed to" or "designed and intended primarily for" standards used for privacy and product safety purposes in the U.S. Inconsistencies increase costs and complexities, and create confusion for consumers.
"Personal Information"/ "Personal Data"	"Personal information" is individually identifiable information about an individual, including contact details (name, address, phone, email, etc.), a persistent identifier that can be used to recognize a user over time and across different online services; a photograph, video or audio file where such file contains a child's image or voice; precise geolocation information (street level), information concerning a child or parent that is combined with another identifier.	"Personal data" is information relating to an identified or identifiable natural person, excluding "anonymous data."	"Personal information" is information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Includes contact details, persistent identifiers, an "alias," characteristics of protected classifications under CA or federal law; biometric information, "geolocation data," audio, electronic, visual, thermal, olfactory or similar information; inferences drawn from any such information.	An "alias," country/city level geolocation information, inference data and other items are not defined as personal information under COPPA or the GDPR. These elements do not allow the physical or online contacting of an individual. Adding inference data, along with household data, is particularly problematic. COPPA requires operators to assume or infer that all users of a website or online service primarily directed to children are under 13. Sites

Requirement	COPPA	GDPR	CCPA	Observations
			Excludes deidentified or aggregate consumer information or publicly available information.	permitted to age-screen under COPPA must likewise assume or infer that those age-screened are under 13.
Persistent/Unique Identifier	A persistent identifier that can be used to recognize a user over time and across different online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number or unique device identifier.	Not defined, but to the extent a persistent identifier relates to an identified or identifiable natural person it is personal data.	Unique identifier or unique personal identifier means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number; unique pseudonym or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device.	The CCPA broadly defines a unique identifier as personal information. Under preemptive COPPA provisions, where persistent identifiers are used solely to support internal operations, parental notice and consent obligations do not apply.
Release; Sale	"Release" of personal information means the sharing, selling, renting, or transfer of personal information to any third party.	N/A	"Sale" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating PI for monetary/ other valuable consideration. Exclusions: • Consumer directs disclosure; • Sharing identifier with third party to confirm opt-out; • Sharing PI with service provider to perform a business purpose if consumer is notified and service provider does not use or sell	COPPA's VPC obligations go beyond those of the CCPA, as they are not linked solely to a "sale."

Requirement	COPPA	GDPR	CCPA	Observations
			PI except to perform the purpose; and • Transfer of PI with a merger, acquisition, or bankruptcy.	
Notice	COPPA is intended to put parents in control of their children's online activities. Operators must post a privacy policy at the home page of the online service and send direct notices to parents in some circumstances. The content of direct notices is subject to specific requirements in § 312.4. Notice and consent obligations do not apply to collection of data through persistent identifiers used solely to support internal operations.	The GDPR framework is based on rights of the data subject. The approach is reflected in the UK ICO Age-Appropriate Design Code. It imposes an obligation to offer age-specific notices to children in relevant formats.	Notify consumers by posting a privacy policy and point of collection notices. Proposed regulations outline detailed disclosure obligations. Update annually. Notify a parent who has affirmatively authorized a "sale" of the right to opt-out and the process for doing so (§ 999.330).	The GDPR, particularly as reflected in the UK ICO Age-Appropriate Design Code, recommends that notices should be provided to the "data subject." The ICO recommends age-specific notices to minors of different age groups (0 -5, 6 – 9, 10 – 12, 13 – 15, 16 – 17) in different formats. COPPA requires notices to parents, since COPPA is grounded in the concepts of parental notice and consent.

Requirement	COPPA	GDPR	CCPA	Observations
Lawful Basis of Processing	Not specifically addressed.	Processing must be based on: • Consent; • Performance of a contract; • Compliance with a legal obligation (under EU law); • Necessary to protect a person's vital interests; • Necessary for performance of a task in the public interest; or • Legitimate interest of the controller.	Not specifically addressed.	Many activities subject to COPPA exceptions can be conducted under the legitimate interest basis of processing under the GDPR. However, the UK ICO draft cookie guidance rejects legitimate interest as a basis for setting any non-essential cookie or technology. This conflicts with the "support for internal operations" exception embodied in the COPPA Rule and may force companies to establish paywalls or other mechanisms to obtain parental consent to conduct basic analytics or perform key business functions.
Limit Data Collection	Operators may not ask a child to provide more information than reasonably necessary to participate in the activity or service.	Only collect and use PI for identified purposes.	Only collect and use PI for identified purposes.	The toy industry supports privacy by design as a key principle of privacy protection.
Responsible Parties	Distinguishes between "operator," "service provider" and "third party." Third party means any person who is not (1) an operator of a website or online service or (2) a person who provides support for internal operations and does not use or disclose PI for any other purpose.	Distinguishes between a "controller," "processor" and "third party": • A controller, alone or jointly, determines the purposes and means of processing; • a processor processes PI on behalf of the controller; • a third party processes PI under the authority of the controller or processor.	Distinguishes between a "business," "service provider" and "third party": • A business, alone or jointly, determines the purposes and means of processing; • a service provider processes information on behalf of a business pursuant to a written contract; • a third party is any person who does not qualify as a business or service provider.	Only a business that "sells" personal information of an individual under 16 is subject to the CCPA parental consent (for those <13) or tween (≥13 – <16) opt-in obligations.

Requirement	COPPA	GDPR	CCPA	Observations
	An operator is strictly liable for data collected at the site or online service.			
Obligation to Oversee Third Party Compliance	Operators may only release children's PI to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of the information and who provide assurances.	Controllers and processors have an independent obligation to comply with the GDPR. Controllers and processors must enter into a contract that includes specific terms set forth in the GDPR.	Businesses, service providers and third parties have an independent obligation to comply with the CCPA. The business and its service providers must have a written contract that prohibits retaining, using, or disclosing PI for any purpose other than as specified in the contract.	
Parental Consent for Data Collection from Children	Yes (< 13), by parent, subject to exceptions.	Yes, by parent if consent is the lawful basis of processing and child is < 16, unless Member State sets different age, which many countries have done.	Yes, by parent if actual knowledge of "sale" of PI from < 13. Proposed regulations state requirements for obtaining affirmative authorization from parents for sale of information of children under the age of 13 are "in addition" to any parental consent requirements under COPPA.	Member States have set different ages (between 13 – 16) for purposes of obtaining parental consent. CCPA requires parental consent for "sale" of PI from individuals <13; such individuals are considered "children."
Opt-In Consent Prior to Sale of PI from ≥13 – <16 Year Old Consumers	N/A	If consent is the legal basis of processing and the individual is under the age of consent in the relevant Member State, consent must be provided by a parent.	A business with actual knowledge that it collects or maintains the PI of individuals ≥13 – <16 must obtain affirmative authorization using a two-step process.	Businesses must get opt-in consent from teens ≥13 – <16 to knowingly sell their data under the CCPA. Treating teens and children identically is not consistent with standard policy recommendations, but some companies will likely require parental consent for any collection or use of information from teens or even all minors to avoid costs of multiple business processes.

Requirement	COPPA	GDPR	CCPA	Observations
"Do Not Sell" Button on Home Page	N/A; but operators may not share or disclose children's PI to third parties, or allow it to be disclosed publicly, without parental consent.	N/A.	Yes; disclosure to service providers excluded from the CCPA "do not sell" requirement.	Sharing with agents and service providers is permitted under COPPA and does not constitute a "sale." Since operators may not "sell" information to third parties for their marketing purposes absent parental consent under COPPA, the CCPA "do not sell" button is inapplicable to child-directed websites.
Honor Opt-Out Requests	Yes. Right to withdraw consent (parent on behalf of child). Operator must verify that requestor is a parent.	Yes. • Right to withdraw consent if consent is the legal basis for processing. • Right to object to processing, unless controller establishes legitimate grounds for processing or for the establishment, exercise, or defense of legal claims. • Right to object to processing for direct marketing. • Right to restrict processing if data subject contests accuracy of the data, the processing is unlawful, controller no longer needs the data, or data subject objects to processing pending confirmation of legitimate grounds.	Yes. Businesses must provide at least two means to exercise choice, *e.g.*, a toll-free number and "Do Not Sell My Personal Information" link on Homepage. "Homepage" means the introductory page and any page where PI is collected. For mobile apps, homepage means the platform page or download page, a link within the app, and any other location that allows consumers to review the notice.	COPPA requires that operator take reasonable steps to confirm requestor is a parent. Authorized agents aren't permitted. Process cannot be overly burdensome for parents.
Honor Right to Access Data	Yes. Upon verification that the individual making the request is the parent, provide:	Yes. Provide: • Purposes of processing; • Categories of PI, recipients/ categories with whom PI shared;	Yes. Disclose categories and pieces of PI collected and third parties with whom PI has been shared during the 12-month period preceding the request.	COPPA requires that operator take reasonable steps to confirm requestor is a parent. Authorized agents aren't permitted. Process

Requirement	COPPA	GDPR	CCPA	Observations
	• A description of types or categories of PI collected; • A means of reviewing the information; and • An opportunity to restrict use or request deletion of child's PI.	• Period for storage; • Right to request rectification or erasure of data, restrict processing, or object to processing; and • Right to lodge complaint with a supervisory authority.	Provide both a toll-free number and a website address, plus an offline method if the primary interaction with consumers is through retail stores. Information must be available at no charge in a portable, readily usable format that allows easy transfer. Not required to provide information to consumer more than twice in a 12-month period. Allow requests to be made by authorized agent.	cannot be overly burdensome for parents. The CCPA requires requests to be verifiable, meaning a request from a consumer, a consumer on behalf of the consumer's minor child, or by an authorized agent. It is not clear if authorized agents may submit a request on behalf of a parent under the CCPA to access or delete information but that conflicts with COPPA. Deletion requests must follow a two-step process, which is inconsistent with COPPA.
Honor Right to Delete Data	Yes, upon verification that the individual making the request is the parent of the child to whom the PI relates.	Yes ("right to be forgotten"), subject to exceptions below, if PI no longer necessary, data subject withdraws consent, data subject objects and there are no overriding legitimate grounds for processing, PI has been unlawfully processed, or PI must be erased to comply with a legal obligation. Guidance, *e.g.*, from the UK ICO, suggests that this right is personal and must be exercised by the data subject (the child).	Yes, subject to listed exceptions. Must use a two-step process for online requests to delete. Allow requests to be made by authorized agent.	See above.
Exceptions to Right to Delete	N/A	No obligation to delete if necessary for: • Exercising right of freedom of expression; • Complying with a legal obligation;	No obligation to delete if necessary to: • Exercise free speech; • Comply with a legal obligation;	

Requirement	COPPA	GDPR	CCPA	Observations
		• Reasons of public interest; • Archiving purposes in the public interest or scientific, historical, statistical research; or • Establishing or defending legal claims.	• Complete a transaction or perform a contract; • Protect against security incidents; • Comply with the California Electronic Communications Privacy Act; • Conduct scientific, historical, or statistical research; or • Conduct internal operations.	
Honor Right to Data Portability	N/A	Yes. Right to receive PI in a structured, commonly used, machine-readable format and right to transfer data to another controller if processing is based on consent or a contract and carried out by automated means.	N/A	
Verify Consumer Seeking to Exercise Rights	Yes. Confirm that person making a request is the parent of the child to whom the PI relates.	Yes	Yes; but allows authorized agents to make requests.	The CCPA requires businesses to honor requests to access or delete personal information from "authorized agents" but appears to also require verification that a "parent" made the request, which is inconsistent. Under COPPA, the operator must ensure that the requestor is a parent of that child, taking into account available technology. Only requests from a parent can be honored.

Requirement	COPPA	GDPR	CCPA	Observations
Timeframe for Responding to Consumer Requests	Not specified	30 days (subject to extension)	45 days (subject to extension)	
Notice to Third Parties	N/A	Yes. Communicate any data subject requests to third parties to whom PI has been disclosed.	Yes. Direct service providers to delete PI upon verifiable consumer request.	
Non-Discrimination	Online services may terminate service to a child whose parent has refused to consent or requested that the operator delete the child's information.	No express provision.	Businesses may not price discriminate against consumers exercising opt-out rights unless difference related to value to the business of the consumer's data. Business may offer financial incentives for the collection of PI.	Operators must refuse or terminate a child's access to a service or portions of a service under COPPA if a child <13 can only access that service with parental consent and a parent fails to consent.
Data Security	Adopt "reasonable procedures" to protect the confidentiality, security, and integrity of PI collected from children. Only release PI to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of the information and provide assurances.	Adopt "appropriate technical and organizational measures to ensure a level of security appropriate to the risk," taking into account the state of the art, costs of implementation, and nature and purposes of processing.	Adopt "reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." Applies to "personal information" as defined in Cal. Civ. Code § 1798.81.5, generally sensitive information.	There is apparent general agreement that security standards must be flexible.

Requirement	COPPA	GDPR	CCPA	Observations
Security Breach Response	N/A.	Controller must notify supervisory authority if a "personal data breach" without undue delay and, where feasible, within 72 hours, "unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons." Controller must notify affected individuals if breach "is likely to result in a high risk to rights and freedoms." Notification is not required if the controller has implemented appropriate security measures or has taken measures to ensure no high risk to data subjects. A "personal data breach" means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."	Breach notifications to affected individuals, state AG, and consumer reporting agencies are governed by existing Cal. Civ. Code §1798.81.5. CCPA allows a private right of action for a consumer whose nonencrypted/nonredacted personal information, as defined in §1798.81.5, is subject to "unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." Before filing suit, a consumer must provide 30 days' notice and an opportunity to cure.	All states and DC have a data breach notification law. Unlike the GDPR, which has uniform data breach reporting obligations for all data controllers, the triggers, timeframes, and required notices for reporting data breaches in the U.S. vary by state. TTA supports a uniform national breach notification standard.

Requirement	COPPA	GDPR	CCPA	Observations
Maintain records of processing	N/A	Yes (information for controller, purposes of processing, categories of data subjects and recipients, transfers to third countries, time limits for erasure, and security measures). Conduct privacy impact assessments. A data protection impact assessment (DPIA) is required where processing is likely to result in a high risk to individuals (*e.g.*, processing children's data)	No general obligation. Proposed regulations require a business with actual knowledge that it collects or maintains the personal information of children under 13 to establish, document and comply with a reasonable method for determining that the person affirmatively authorizing the sale of PI about the child is the parent or legal guardian.	
Conduct Training	N/A	N/A	Ensure that all individuals responsible for handling consumer inquiries are informed of all requirements.	
Restrict Transfers to Countries with Adequate Privacy Laws	N/A	Yes, using an approved mechanism.	N/A	
Penalties	$40,000 per violation. No private right of action.	Up to 2% annual global turnover or €10 million (whichever is greater), or up 4% annual global turnover or €20 million (whichever is greater), depending on violation. Private right of action.	AG can impose penalties of $2,500 per violation ($7,500 per intentional violation) if not cured within 30 days after being notified by the AG. Private right of action limited to violations of §1798.81.5 (CA security breach law). Plaintiff can recoup the greater of actual damages or $100 - $750 per incident. Plaintiff must provide 30 days written notice.	