



Inspiring Generations of Play

1200 G Street NW • Suite 200 • Washington, DC 20005

t. 202.459.0354 • e. info@toyassociation.org

December 21, 2018

Via Electronic Submission at <https://www.regulations.gov/comment?D=FTC-2018-0098-0003>

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Hearings on Competition and Consumer Protection in the 21st Century—Consumer Privacy and Data Security (Docket No. FTC-2018-0098)

The Toy Association, Inc., on behalf of its members, appreciates the Federal Trade Commission’s (FTC) thoughtful attention to consumer privacy and data security, and we hope this submittal will assist the Commission as it prepares for its February 12–13, 2019, Hearings on Competition and Consumer Protection in the 21st Century.

Few industries are as heavily regulated as the toy industry. From privacy to product safety, industry members are heavily regulated by an extensive set of preemptive laws. Thus, the toy industry is uniquely qualified to comment on consumer privacy and data security issues. The Toy Association hopes to be an active partner in discussions regarding consumer privacy and data security while ensuring that existing effective sectoral laws like the Children’s Online Privacy Protection Act (COPPA) are retained.

While technologies and business models have changed significantly since the FTC issued its last comprehensive privacy report in 2012, the Commission’s work to review and update COPPA over the years has resulted in a remarkably resilient regulatory regime that is widely acknowledged to be both effective and reflective of technological developments. COPPA, last amended in 2013 (78 Fed. Reg. 3,971 (Jan. 17, 2013)), has managed to stand the test of time even as technology rapidly changes, making it an excellent model for a general privacy and data security framework. While many aspects of COPPA, such as its notice and parental consent requirements, are clearly tailored to protect the interests of children and would not be appropriate for general legislation, other aspects, such as the exceptions for collection of persistent identifiers used solely to support internal operations, reflect a common-sense harms-based approach to privacy that balances limited potential risks to individuals with a recognition of business needs and consumer convenience.

In amending COPPA’s definition of “personal information” to include persistent identifiers used over time *and* across websites, for example, the FTC recognized both that the sensitivity of such information is highly correlated to its use and that universally categorizing such data as “personal” would be both unwise and operationally unworkable. Thus, while use of persistent identifiers for behavioral targeting purposes is not permitted, the final Rule allows collection and use of persistent identifiers to support a number of essential business activities, such as basic functionality and general data analytics, among others. Accordingly, the final rule exempts data collected solely to support an online service’s internal operations.

Under the Rule, support for the internal operations of a website or online service 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;

so long as the information collected for the activities listed in paragraphs (a)-(g) 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. Support for internal operations also includes activities such as intellectual property protection, payment and delivery functions, spam protection, optimization, statistical reporting, or de-bugging. *See* 78 Fed. Reg. at 3,981.

Since the Rule was adopted, the FTC has clarified that it applies to all online services directed to children under 13, including apps and connected products. *See* FTC, *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, available at <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>. The FTC has also adopted some common-sense enforcement positions reflective of technological advancements. For example, while the Rule technically requires parental consent before an online operator can collect audio recordings of children's voices, the FTC staff has made clear that brief collection of audio files to perform functions, such as a search or to fulfill a verbal instruction or request, would not be the target of enforcement action so long as the file is held for a brief time and used only for basic functionality. *See* FTC, *FTC Provides Additional Guidance on COPPA and Voice Recordings*, available at <https://www.ftc.gov/news-events/press-releases/2017/10/ftc-provides-additional-guidance-coppa-voice-recordings>.

Most online services cannot function without some limited data collection, but COPPA recognizes that that collecting and sharing certain information – particularly information that could result in exposure of a child's contact information to third parties - potentially creates a higher risk to children's privacy. COPPA includes interventions, such as parental notification and consent obligations, designed to assure that parents are notified and, where appropriate, consent to certain types of information collection and use. Moreover, COPPA's sliding scale approach to consent recognizes that the most robust forms of parental consent should be reserved for situations where privacy harms are potentially greater. Implementing this type of harms-based approach results in a framework that is crafted to better assure their efficacy in addressing risks, and the underlying concepts could be applied to general privacy legislation.

Just as privacy protections should be designed with the user's age in mind, they should also bear in mind the type of collection, processing, and eventual use of specific categories of data collected, with due regard for the potential harm associated with use and misuse. For instance, the interventions designed to protect young children's (those under 13 years of age) privacy, would not be effective for teens, who have their own evolving sphere of privacy. The Toy Association believes that any general legal regime governing privacy must recognize that privacy rights and risks relate to the sensitivity of the data, with special protections for certain types of data. Health data and financial data, like children's data, deserve enhanced protection.

The Toy Association continues to support COPPA and its members maintain a strong commitment to safeguarding children's personal information. Accordingly, the COPPA framework and its essential definitions should be kept intact. Any future general privacy and data security legislation should ensure that key concepts and definitions do not conflict with those found in COPPA, but rather should build on COPPA's fundamental harms-based approach. Finally, it is likewise essential that the preemptive framework of COPPA be maintained. Our industry can ill afford new privacy and data security legislation that undermines the proven effectiveness of a statute like COPPA while making compliance considerably more challenging and expensive and the user experience less desirable.

With these thoughts in mind, we share the attached comments that were submitted in response to the National Telecommunications and Information Administration's (NTIA) notice and request for public comments (RFC), 83 Fed. Reg. 48,600 (Sept. 26, 2018), seeking information on ways to protect privacy while fostering innovation. These comments provide greater detail on the Toy Association's position regarding future privacy and data security legislation, and we hope the FTC will find them helpful.

We appreciate the opportunity to share these views. Please contact Ed Desmond at edesmond@toyassociation.org in our Washington, DC office if you would like additional information on our industry's perspective.

Sincerely,


Steve Pasierb
President & CEO

Enclosure

ATTACHMENT

Toy Association, Inc. Comments

National Telecommunications and Information Administration (NTIA)

Developing the Administration's Approach to Consumer Privacy

[Docket No. 180821780-8780-01]



November 9, 2018

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230
privacyrfc2018@ntia.doc.gov

Re: Developing the Administration's Approach to Consumer Privacy [Docket No. 180821780-8780-01]

The Toy Association, Inc., on behalf of its members, is pleased to submit these comments in response to the National Telecommunications and Information Administration's (NTIA) notice and request for public comments (RFC), 83 Fed. Reg. 48,600 (Sept. 26, 2018), seeking information on ways to protect privacy while fostering innovation. Because of the extensive set of preemptive laws that govern children's privacy and toy safety, the toy industry is uniquely qualified to comment in response to this RFC.

By way of background, The Toy Association represents more than 950 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. Our members not only create toys that are safe to physically play with, but many members offer websites and apps with games and activities for children, connected toys that allow kids to leverage the power of the Internet to enhance physical play, and e-commerce and other opportunities for adults. Protecting children and maintaining the trust of parents are the most vital concerns for the toy industry. The Toy Association and its members believe that protecting consumer privacy while fostering innovation and choice in the marketplace reflect core American values. Fair information practice principles, such as transparency, security, data minimization, and privacy by design and default, are central values for toy companies handling consumer personal data, especially when the consumer is a child. Reflecting these values, The Toy Association supports the goal of a uniform federal privacy framework that retains existing strong and effective national safeguards. In that regard, the Children's Online Privacy Protection Act (COPPA), in force for two decades, has made the U.S. the global leader in protecting children's privacy, and could serve as a model for a uniform national approach.

Most importantly for purposes of this RFC, child-directed online services, including connected children's toys, are subject to strict requirements under COPPA, which already addresses the RFC's core privacy outcomes. While the Toy Association recognizes that many other sectors are not subject to the same requirements and standards as the toy industry, the current system of federal preemptive laws governing children's privacy, health privacy and financial privacy has worked well to protect consumers. These existing systems, and the sectoral laws and definitions that come with them, should be respected as businesses have spent decades and significant resources to build compliant systems and processes. Thus, we discourage the development of new frameworks that seek to unnecessarily replace existing models that work well. In particular, it is crucial that legislation avoid adopting new definitions for key terms and concepts that do not track with existing laws and interpretations. It is equally important that privacy laws avoid elevating form over substance by requiring burdensome documentation and certifications, or fostering unnecessary litigation.

The U.S. should promote a robust system of uniform, national privacy grounded in real potential privacy and information security risks and harms, not imitation of state or international legal frameworks like the California Consumer Privacy Act (CCPA) or the EU General Data Protection Regulation (GDPR). The toy industry recommends that a federal privacy framework reflect the following principles:

- **A federal privacy framework should be uniform, flexible, technology-neutral, consistent with existing successful laws, and risk-based.**

The Toy Association appreciates NTIA's thoughtful approach to promoting consumer privacy. We concur that any approach to protecting privacy should be flexible and based on risks and benefits. The goal of any federal privacy framework should be to broadly address privacy and security to avoid the inevitable disruption and confusion which will come from a patchwork of inconsistent state laws or failure to recognize the preemptive effect of existing laws. . To avoid duplication, a risk-based, technology-neutral, process-management oriented approach that builds on existing federal privacy and security frameworks and requirements is desirable.

We believe this is preferable to unduly proscriptive approaches that may degrade user experiences, impose unnecessary burdens on business, and create confusion for all. With the adoption in California of problematic legislation that is likely to have these results, it is increasingly important for the U.S. to have a uniform federal framework that is broadly applicable without undermining existing laws. In developing an approach, it is important to consider differences between platforms, types of data collected, the potential sensitivity of data, technologies used, types of user experiences offered, consumer convenience and benefits, promoting innovation, practical implications for back-end data management, existing legal requirements, and the important role for self-regulation.

- **The definition of a "child" should not be altered.**

The COPPA definition of a "child" as those under 13 has been the cornerstone of the U.S. approach to children's privacy since COPPA was enacted twenty years ago. A key part of COPPA is the requirement that operators of websites and online services obtain parental consent before they collect certain types of information from children under 13 if their online services are primarily directed to children, or if they have actual knowledge that they collect personal information from children under 13. This definition is consistent with how a "children's product" is defined in the Consumer Product Safety Improvement Act (CPSIA). *See* 15 U.S.C. § 2052(a)(2). It is crucial to the toy industry that regulatory frameworks ensure consistency of these definitions, particularly for connected toys that will be regulated under both. Adoption of age 13 is likewise consistent with international recommendations on how "children" should be defined from a privacy perspective. *See* International Chamber of Commerce (ICC) Toolkit: Marketing and Advertising to Children, available at <https://iccwbo.org/publication/icc-toolkit-marketing-advertising-children/> .

COPPA recognizes that parents are best-equipped to determine the types of online interactions that are suited to the needs of children under 13, but also recognizes that some types of interactions present small or no privacy risks and do not require consent. Moreover, age 13 was selected because teens have a growing sphere of privacy, and parental consent mandates are unlikely to be effective with teens. Up-aging has significant adverse regulatory consequences, potentially leading to inconsistencies in how physical toy safety and informational safety are regulated. Likewise, altering the definition of a "child" can greatly complicate when a firm might have "actual knowledge" that they are dealing with someone under age. Frameworks like the GDPR, which allow Member States to define a "child" as an individual between 13 and 16, simply create confusion, rather than foster an appropriate privacy framework.

Toy industry members support fair information practice principles, such as data minimization, transparency, security, and access, correction and deletion rights. COPPA provides a harms-based, sensible approach to privacy that balances protecting children's privacy against overly burdensome obligations on parents and

businesses, and the toy industry recommends it as a model in crafting any framework that seeks to promote consumer control over privacy.

- **The FTC should be designated as the primary enforcer of consumer privacy and information security.**

Because of its extensive experience with existing data and security issues, including enforcement of COPPA, the toy industry supports designating the Federal Trade Commission (FTC) as the appropriate federal agency to enforce consumer privacy for most sectors. The FTC’s authority under Section 5 of the FTC Act is sufficient to support the agency’s future activities in this area; however, we also agree that the FTC would benefit from increased resources.

- **New privacy frameworks should maintain a strong role for industry self-regulation and industry education.**

The Toy Association believes it is important that any new federal privacy framework encourage self-regulation, much as the current COPPA framework promotes self-regulation. Those of our members that participate in approved COPPA Safe Harbor programs have confirmed the benefits of that participation in offering additional review and opportunity to explore new ways to protect privacy and, where appropriate, to seek parental consent. When a complaint is lodged about practices of a member of a recognized Safe Harbor program, it should be referred to the Safe Harbor organization first for resolution. While it is difficult to develop one-size-fits-all privacy requirements, self-regulatory bodies geared to the sector they work with are designed to address the unique needs of their participants.

Trade organizations and other industry groups are also well-suited to promoting privacy and data security, and The Toy Association’s activities are a perfect example. The Toy Association has provided COPPA compliance resources for its members. The Toy Association and its members also support these five guiding principles to ensure the privacy, safety and security of connected toys: Safety by Design; Privacy First; Safeguarding Security; Transparency; and Empowering Parents and Caregivers. These principles illustrate that there are indeed some privacy concepts that can be generally applied to protect consumers, but there must be room for industry to tailor approaches and address unique challenges.

* * *

The toy industry remains deeply committed to supporting sound technical and policy practices and solutions to tackle potential threats to privacy. We look forward to being a productive part of future discussions regarding consumer privacy while ensuring that existing effective laws like COPPA are retained.

If you would like to follow up with us contact Ed Desmond at edesmond@toyassociation.org in our Washington, DC office.

Sincerely,



President & CEO