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

In the Matter of

Request for Public Comment on the	**)**
Federal Trade Commission's	**)**
Preliminary Staff Report,	**)**
Protecting Consumer Privacy in an	**)**
Era of Rapid Change: A Proposed	**)**
Framework for Business and	**)**
Policymakers	**)**
	)

COMMENTS OF THE TOY INDUSTRY ASSOCIATION

February 18, 2011

In the Matter of

Request for Public Comment on the	**)**
Federal Trade Commission's	**)**
Preliminary Staff Report,	**)**
Protecting Consumer Privacy in an	**)**
Era of Rapid Change: A Proposed	**)**
Framework for Business and	**)**
Policymakers	**)**
	)

COMMENTS OF THE TOY INDUSTRY ASSOCIATION

INTRODUCTION

The Toy Industry Association ("TIA") is pleased to submit these comments in response to the Federal Trade Commission's ("FTC" or "Commission") request for public comment on its "preliminary" staff privacy report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers* ("FTC Report" or "Privacy Report").[1] The FTC has requested comments on its proposed framework, in an effort to further develop and refine the framework for its final report.

BACKGROUND

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

TIA members are in the business of creating fun, safe toys for children. As a natural extension of that business, our members are committed to offering entertaining, educational, safe online environments for children. Many of our members host websites that offer games, activities and features for children, and some offer online content for teen and adult collectors. In addition, TIA members may host online stores where parents can shop for products. Trust and confidence of parents is central to our industry, so respecting the privacy of all customers is a core value for TIA members.

The FTC noted in its Report to Congress that the Children's Online Privacy Protection Act of 1998 ("COPPA")[2] "has provided a workable system to help protect the online safety and

[1] *See* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[2] 15 U.S.C. §§ 6501-6508.

privacy of the Internet's youngest visitors."[3] We agree. Our concern is some of the generalized concepts in the Privacy Report do not take into account legal, policy, operational and practical issues. In particular, we note inconsistencies between aspects of the proposed framework and COPPA.

COMMENTS

It is critical that any new recommendations affecting privacy in general avoid conflicting with existing privacy laws, including, in particular, the requirements of COPPA and the COPPA Rule.[4] Put simply, apart from the broader questions of the effectiveness of a "Do Not Track" database, a database of individuals known to be children under 13 cannot be implemented under COPPA currently because the creation of such a database requires verifiable parental consent. It is critical that any changes to COPPA and/or to general privacy practices be developed considering the broad legal and practical implications, including those on companies who operate websites or online services directed to children. The FTC should not move forward on its COPPA Rule Review[5] without thoroughly evaluating the responses to similar questions raised in this proceeding.

As discussed in detail during the COPPA Rule Review, TIA's members remain deeply concerned with expanding application of COPPA to data that is simply linked to a device identifier like an IP address. Doing so actually *undermines* the legal framework of COPPA, which was predicated on a careful distinction between personal information and non-personal information. Eliminating that distinction could potentially require the collection of more information – including information that many parents would view as "sensitive" – than currently is collected by many child-oriented websites, built to operationalize COPPA's legal distinction between personal and non-personal information. TIA also believes that the verifiable parental consent mechanisms currently recognized in the COPPA Rule pose a legal and operational barrier to adopting a mandatory Do Not Track mechanism.

President Obama's recent Executive Order stressed the need for agencies to reduce burdens, urging that agencies "identify and use the best, most innovative, and least burdensome tools for achieving regulatory ends...[and] must measure, and seek to improve, the actual results of regulatory requirements."[6] Unnecessary expansion of regulation, or new requirements that adversely affect existing laws and regulations that work well, must be avoided. To the extent aspects of the Privacy Report react to online behavioral advertising (OBA) concerns, it is also vital to recognize the self-regulatory initiatives in place to address OBA and provide more transparency.

---

[3] Federal Trade Commission, *Implementing the Children's Online Privacy Protection Act: A Report to Congress* at 28 (February 2007), http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf.

[4] Children's Online Privacy Protection Rule, 16 C.F.R. Part 312.

[5] *Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule*, 75 Fed. Reg. 17,089 (April 5, 2010).

[6] Executive Order 13563 (January 18, 2011).

The FTC has posed a series of important questions, and we provide responses to several specific questions.

Is it feasible for the framework to apply to data that can be "reasonably linked to a specific consumer, computer, or other device"? If it is not feasible, what alternatives exist?

FTC proposes that its framework should not be limited only to those who collect personally identifiable information ("PII"). Rather, the framework would apply to commercial entities collecting data that can be reasonably linked to a specific consumer, computer, or other device. To the extent this framework would apply to all data, including children's data, the FTC would essentially do away with the traditional distinction between PII and non-PII that is fundamental to the legal framework of COPPA. This distinction has been the foundation of a successful system that the FTC itself has repeatedly indicated does protect the privacy of children online. Data linked to personal information, such as an e-mail address, of a child under 13 is fully subject to the COPPA framework. However, data linked to a device or computer identifier is not.

FTC advises that support for eliminating this distinction came from various roundtable participants, who believe that the "traditional distinction between PII and non-PII continued to lose significance due to changes in technology and the ability to re-identify consumers from supposedly anonymous data."[7] However, the ability to contact someone directly is the underpinning for the categories of information considered to be "personal information" under COPPA. As indicated in TIA's comments on the COPPA Rule, creating a new privacy framework that eliminates distinctions between personal and non-personal data in all cases represents a sea change in COPPA. The result will be to require companies to collect even *more* information from a child, such as a child's e-mail address and parent's e-mail address, as soon as a visitor comes to a site, to comply with COPPA's parental notice and consent requirements.

TIA continues to believe that protecting privacy requires consideration of many factors, such as the type and degree of sensitivity of data, reasons for collection and use, existing legal requirements, optimizing the user's experience, and minimizing regulatory burdens, to name a few. Close consideration should be given to how self-regulatory approaches in areas currently not regulated, such as the general practice of OBA, can address concerns. FTC proposes to provide consumers choice over collection and use of data regarding their online searching and browsing activities through a mechanism called "Do Not Track." This mechanism would involve the placement of a setting similar to a persistent cookie on the consumer's browser. This "cookie" would convey the consumer setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements. This Do Not Track mechanism would be used to ensure that consumers would not have to exercise choices on a company-by-company or industry-by-industry basis, noting that such choices would be persistent. The FTC has rejected a mandated "Do Not Track" feature on child-directed websites absent verifiable parental consent under COPPA. The conundrum presented by the FTC's choice

[7] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers*, at 43 (December 2010).

concept is that creating such a database could require collecting more information from parents and children to create such a database.

What technical measures exist to "anonymize" data and are any industry norms emerging in this area?

For companies invested in protecting children's privacy, the current COPPA framework is predicated on a presumption of promoting an interactive experience while protecting children's privacy through collection of information considered to be anonymous. Age, zip code, gender, a user name and password, and an IP address, for example, may be collected to offer age-appropriate content or obtain general demographic information. That information can be important to toy companies in both updating website content and in product development. Importantly, this type of information *is* deemed anonymous under COPPA when it is not linked to an identifier, such as an e-mail address, that allows an individual to be directly contacted online or offline.

This prompts several questions. What sort of additional "anonymization" is the FTC contemplating? How will general "anonymization" requirements affect current practices and approaches that are mandated or permitted under COPPA? What operational changes will be required as a result? How will that affect the user's experience? Changes could result in significant operational impacts on companies involving practices that have little practical implication for children's privacy.

Are there practical considerations that support excluding certain types of companies or businesses from the framework – for example, businesses that collect, maintain, or use a limited amount of non-sensitive consumer data?

Of course reasonable exemptions should apply, and context of collection and use is important to defining exemptions. The COPPA regime, for example, covers online collection of *personal* information from children, but also recognizes some exemptions, even though collection of personal information from children may be deemed "sensitive." For example, some limited personal information, like an e-mail address, can be collected from children in specific circumstances. Where additional personal information is needed to permit participation in a site or activity, parental consent is obtained. These legal activities may be adversely implicated by a general privacy framework that eliminates distinctions or fails to acknowledge common sense exclusions. It is important to remember, for example, that certain information, like an IP address, is logged because it may help in an assessment of risk of security breaches, malware, or fraud. Certain types of personal information are subject to specific exemptions under COPPA, discussed below, relevant to the types of "commonly accepted practices" that merit exclusions from this framework. COPPA recognizes that not every item of even personal data is equally sensitive.

Is the list of proposed "commonly accepted practices" set forth in Section V(C)(1) of the report too broad or too narrow?

The FTC has identified the following "commonly accepted practices," for which companies do not need to provide "choice" because data collection is expected: 1) product fulfillment, 2) internal operations, 3) fraud prevention, 4) legal compliance and public purpose, and 5) first-party marketing. This list is not necessarily completely congruent with COPPA, and thus appears to be overly narrow. The COPPA rule, for example, permits collection of personal information, such as online contact information of a child, to the extent reasonably necessary to protect the safety of a child at the website or online service, to protect the security or integrity of a website or online service, to take precautions against liability, to respond to judicial process, or, to the extent permitted, to provide information to law enforcement agencies or for an investigation on a matter related to public safety. Consistent with COPPA, choice should not be needed for actions that relate to responding to potential threats to the physical security of an individual, or investigating threats to personal or intellectual property or the security of business or personal data, which fall short of "fraud." "Internal operations" presumably includes sharing with agents or other service providers.

What (if any) special issues does the collection or the use of information about teens raise? Are teens sensitive users, warranting enhanced consent procedures? Should additional protections be explored in the context of social media services? For example, one social media service has stated that it limits default settings such that teens are not allowed to share certain information with the category "Everyone." What are the benefits and drawbacks of such an approach?

The topic of protecting teens was discussed during workshops on COPPA last summer. A parental consent process is unlikely to be workable or practical with teens.

What is the feasibility of standardizing the format and terminology for describing data practices across industries, particularly given ongoing changes in technology?

TIA members do strive to offer readable, comprehensible and comprehensive privacy policies that address offerings for adults and children. The content of privacy notices for websites or areas of websites directed to children is mandated by COPPA, however. The standardized terminology of COPPA, required to be repeated in notices to parents, is not the best model to replicate. Privacy policies are not like boxes of cereal. Different business practices and different technologies may merit different types of consumer disclosure. Context matters. While improved communications are to be encouraged, standardized terminology and even formats risk freezing technology and may not keep pace with new devices or technology. There are inherent tension between simplified notices and complete transparency, especially given prior FTC statements that "short" privacy policies may not be inconsistent with "complete" versions. The use of icons merits some exploration, but these notice techniques are currently not permitted under COPPA.

CONCLUSION

TIA members are committed to protecting the privacy of all consumers, especially children. Many of the questions raised by the FTC here are similar to those raised in the COPPA proceeding. TIA and its members have a unique perspective on COPPA so appreciate the opportunity to submit these comments.

Respectfully Submitted,

Carter Keithley
President

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