Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of	)	
	)	
COPPA Rule Review, 16 CFR Part 312	)	Project No. P104503
	)	
	)	

COMMENTS OF THE
MOTION PICTURE ASSOCIATION OF AMERICA, INC.

MOTION PICTURE
ASSOCIATION OF AMERICA, INC.
Michael O'Leary
Senior EVP, Government Relations
Linda Kinney
Vice President, Regulatory Affairs
1600 Eye Street, NW
Washington, DC 20006
(202) 378-9139

December 23, 2011

TABLE OF CONTENTS

Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of	)	
	)	
COPPA Rule Review, 16 CFR Part 312	)	Project No. P104503
	)	
	)	

COMMENTS OF THE
MOTION PICTURE ASSOCIATION OF AMERICA, INC.

The Motion Picture Association of America, Inc. ("MPAA")[1] hereby submits these comments in response to the Federal Trade Commission's ("FTC" or "Commission") Notice of Proposed Rulemaking ("*Notice*") regarding implementation of the Children's Online Privacy Protection Act ("COPPA").[2] The MPAA and its member companies are strongly committed to protecting the privacy and safety of children in the digital world.[3] Thus, the MPAA and its members look forward to continuing to work with the FTC, industry, and children's advocacy groups to ensure that COPPA's existing protections are implemented in a manner that protects children, while allowing them to benefit fully from the wide range of valuable content available on the Internet.

---

[1] The MPAA, together with the Motion Picture Association ("MPA") and MPAA's other subsidiaries and affiliates, serves as the voice and advocate of the American motion picture, home video, and television industries in the United States and around the world. MPAA's members are the six major U.S. motion picture studios: Walt Disney Motion Pictures Studios; Paramount Pictures Corporation; Sony Pictures Entertainment Inc.; Twentieth Century Fox Film Corporation; Universal City Studios, LLC; and Warner Bros. Entertainment Inc.

[2] Proposed Rule; Request for Comment, 76 Fed. Reg. 59804 *et seq.* (Sept. 27, 2011) ("*Notice*"); COPPA Rule, 16 CFR Part 312, issued pursuant to COPPA, 15 U.S.C. § 6501 *et seq*.

[3] As discussed in more detail herein, MPAA companies were early supporters of COPPA, and MPAA has participated in and commented on previous reviews of the COPPA Rule.

I. INTRODUCTION AND OVERVIEW

The Internet offers children and their parents access to an expanding universe of educational and entertainment content. On MPAA member sites, children and families can view episodes of their favorite programming; create art based on such programming; play educational and entertaining games; and even participate in virtual worlds where they can interact with peers in protected environments.

Children's advocacy groups, policymakers, and website operators all agree that encouraging parental involvement in the online activities of their kids is the best way to protect young children on the Internet. MPAA members are investing significant resources in new technologies and a wide range of tools to help parents monitor and guide their children's online activities.[4] Flexibility to craft a variety of safety measures is essential, however, so that operators can ensure that such measures are appropriate for a particular age group and tailored to certain types of games and activities. A one-size-fits-all approach would limit rather than promote creative ways to keep kids safe online.

The Commission's current COPPA rules strike a workable balance between the privacy and safety of young online users and access to the latest innovative content. The issues raised in this rulemaking proceeding do not address any identified harm to children that has arisen from any gaps in the COPPA Rule. Thus, the MPAA agrees with the Commission's assessment that the current age threshold and use of the "actual knowledge" standard should be retained. However, the broad proposals to make the definition of "personal information" more expansive are unnecessary and do not address any specifically identified harm to children that is occurring

[4] *See* Pause Parent Play, http://www.pauseparentplay.org/ (last visited Dec. 21, 2011). Pause Parent Play is a coalition dedicated to helping parents choose which video games their children play, among other things. MPAA is a member of the coalition. *See* Parent Resources, MPAA, http://mpaa.org/parentsresources (last visited Dec. 21, 2011). *See also* MPAA Comments RE: COPPA Rule Review P104503 (filed Jul. 12, 2010) ("MPAA 2010 Comments") at 3-4.

under the current version of the COPPA Rule. Moreover, these proposals conflict with congressional intent and exceed the authority granted to the FTC by the statute.[5] Website operators should have the flexibility to collect and use data that enhances a child's online experience, provided such use does not pose a safety threat. Consistent with the plain language of COPPA, we urge the Commission to exercise restraint by limiting the definition of personal information to information that "permits the physical or online contacting of a specific individual."[6] In any event, the Commission should state explicitly that any changes to the COPPA Rule adopted in this proceeding apply only to websites covered by COPPA and do not implicate non-COPPA sites.

II. BACKGROUND

A. SAFEGUARDS AND PARENTAL TOOLS

MPAA companies commit significant resources to online safety, employing multiple privacy professionals to design and operate COPPA compliant sites. MPAA members are investing in sophisticated filtering technology, often augmented by appropriate levels of human monitoring and review, depending upon the particular circumstances, to prevent the collection or disclosure of personally identifiable information from children under 13. A variety of mechanisms are used to secure verifiable parental consent under the sliding scale, which permits businesses to secure parental consent through cost-effective mechanisms that are appropriately tailored to a particular setting. In some cases, MPAA members facilitate interactivity without collection or disclosure of personal information, for example by offering registration and

[5] As discussed in detail herein, the MPAA does not believe that such modifications to the Rule are necessary. However, if the FTC modifies the COPPA rule in the instant proceeding, parties should be afforded substantial time to adjust their practices in order to come into compliance.

[6] 15 U.S.C. § 6501(8)(F).

personalized content tied to unique screen names or other information that contain no personally identifiable information.

One way website operators have bolstered online safety is by hiring personnel to monitor chat rooms and review screen names to ensure they do not contain email addresses that would allow strangers to contact individual children. Other websites restrict "chat" features to protect children. For example, to ensure that no personal information is divulged inadvertently, some websites use sanitized dictionaries that do not include numerals, spelled out digits, or individual letters; do not include street names, city names, or state names; prevent use of the words "street," "lane," "road," or "boulevard"; and include only proper first names of popular characters. In addition to the sanitized dictionary, users can block other visitors from chatting with them and can report any incident directly. Parents can further restrict chat by only allowing chats from certain friends or by limiting the use of a pre-written set of messages.

Another creative approach is to offer two "chat" settings for children in certain games and virtual worlds: one that allows the use of only pre-selected phrases, and one that allows users with parental approval to write custom messages, but prohibits certain words and phrases, including some categories of personally identifiable information such as phone numbers. Some website operators also use filtering technology on the chats. Other sites offer tools for parents to monitor their child's use of the chat feature in virtual worlds.

B. THE CURRENT RULES HAVE BEEN EFFECTIVE

Consistent with the plain language of the statute and Congress's intent, the Commission determined in 1999 that screen and user names, persistent identifiers, and photographs could be personal information only when combined with other individually identifiable data. The Commission's sound exercise of judgment on this question a dozen years ago, and again in 2006, has permitted site operators to use anonymous screen names, user names, and persistent

identifiers flexibly to customize and enrich children's online experiences, and permit children to post pictures and other creative work without compromising their privacy. Screen names and user names, for example, are integral to the games and other interactive online activities that have special appeal for children. On feature-rich MPAA member sites that let users participate in virtual worlds or interact socially, anonymous user names and screen names facilitate login and permit users to locate each other. Even on simple game sites that do not include virtual worlds or social interaction, user names and other anonymous login data permit users to keep track of high scores and points used, and enable other user customization. For user convenience and to eliminate the need for multiple registrations and logins, some site operators permit users to adopt a single user name or screen name to be used across different sites controlled by the same operator, or to use a single user name or screen name on multiple platforms, such as computers or mobile devices.

In sum, website operators have employed a variety of creative tools to promote a safe online environment for kids by embracing innovation and new technology. Safety measures are often crafted for a certain type of game, activity or age group to ensure that they are both appropriate and tailored. In the past, the FTC has recognized the importance of flexibility and has found that safeguarding children does not require an over-regulatory, one-size-fits-all approach.[7]

[7] *See Notice* at 59819.

III. DISCUSSION

A. THE COMMISSION CORRECTLY PROPOSES TO RETAIN THE PRESENT AGE THRESHOLD AND THE "ACTUAL KNOWLEDGE" STANDARD

1. THERE IS NO BASIS FOR EXTENDING COPPA'S PROTECTIONS TO CHILDREN AGE 13 AND ABOVE

Although teenagers clearly face certain privacy challenges online,[8] the Commission is correct to conclude that the statutory definition of a "child" to mean any person age 12 or under remains appropriate today.[9] In 1998, Congress and the FTC appropriately decided that COPPA's protections should not cover adolescents over the age of 12.[10] In revisiting the issue in this proceeding, the Commission again concluded that, from a practical perspective, COPPA's parental notice and consent approach is far more likely to be successful for young children than for teenagers.[11] The MPAA agrees with this assessment and applauds the Commission for recognizing the difficulties of implementing the COPPA model for teenagers, who may be more inclined to falsify parental or age information in order to participate in online activities.[12] We

---

[8] *See id.* at 59805.

[9] COPPA and the FTC's COPPA Rule define a "child" to be "an individual under the age of 13." 15 U.S.C. § 6502(1); *Notice* at 59805; Protecting Youths in an Online World: Hearing Before the Subcomm. on Consumer Protection, Product Safety, and Insurance of the Senate Comm. on Commerce, Science & Transportation, 111th Cong. 14-15 (2010) (Statement of Jessica Rich, Deputy Director, Bureau of Consumer Protection, Federal Trade Commission), *available at* http://www.ftc.gov/os/testimony/100715toopatestimony.pdf.

[10] When it enacted COPPA, Congress specifically considered whether to include a requirement tailored to children ages 13 to 17; however, it ultimately defined a "child," for purposes of the statute, to be under the age of 13. *See Notice* at 59805; *Children's Online Privacy Protection Act of 1998*, S. 2326, 105th Cong. § 3(a)(2)(iii) (1998) (requiring that operators use reasonable efforts to provide parents with notice and an opportunity to prevent or curtail the collection or use of personal information collected from children over the age of 12 and under the age of 17). The Commission supported this distinction between older children (ages 13 to 17) and younger children (under age 13), who may not be fully capable of understanding the consequences of sharing personal information online. Based on input from advocates, educators, and industry, Congress's decision reflected the collective judgment that extending the covered age range above 12 would impact too many general-audience web sites, at too great a cost in terms of both access to content and the emerging digital economy, without offsetting benefits. As MPAA explained in its initial comments, this equation has not changed in the 13 years since COPPA was enacted.

[11] *See Notice* at 59805. As discussed in the *Notice*, numerous commenters "expressed concern that expanding COPPA's coverage to teenagers would raise a number of constitutional, privacy, and practical issues." *Id.*

[12] *See id.*; *see also* Comments of Center for Democracy and Technology ("CDT") at 5 (definition of child as an individual under age 13 focuses the scope of the Rule properly on younger minors).

also concur with the Commission's conclusion that expanding COPPA's reach could unintentionally burden the right of adults to engage in online speech and could reduce teenagers' access to valuable online services.[13] For these reasons, MPAA strongly supports the conclusion in the *Notice* that COPPA should continue to apply to children under the age of 13 and that COPPA is not the appropriate vehicle to address teen online privacy issues.

2. ANY STANDARD OTHER THAN ACTUAL KNOWLEDGE WOULD CAUSE HARM WITHOUT COUNTERVAILING BENEFITS

MPAA also agrees with the Commission that COPPA should continue to apply only to "the finite universe of websites and online services directed to children and [general audience] websites and online services *with actual knowledge*" that they are collecting personal information from a child under age 13.[14] While some websites operated by MPAA members are directed to children, others are intended to be accessed by a more general population of all ages, with an interest in the motion picture industry or specific programs, movies, or games. For websites in this latter category, only the existing "actual knowledge" standard would provide sufficient clarity to the operator. Otherwise, the site might need to be programmed to "guess" a user's age[15] or to collect far more information than actually is necessary.[16] MPAA thus supports

---

[13] *See Notice* at 59805; Comments of CDT, Progress and Freedom Foundation ("PFF"), and Electronic Frontier Foundation ("EFF") at 8-10 (expanding COPPA would subject sites that cater to both adults and children to COPPA's parental consent requirements, and would violate the First Amendment); Comments of the Promotion Marketing Association ("PMA") at 5 (increasing the applicable age of COPPA not only requires drastic restructuring of online access, but would also limit access by those of an appropriate age, implicating their First Amendment rights).

[14] *Notice* at 59806 (emphasis added).

[15] *See, e.g.,* Comments of the Interactive Advertising Bureau ("IAB") at 6.

[16] *See, e.g.,* Comments of CDT, PFF, and EFF at 7 (explaining that under a constructive knowledge standard, operators would not have a clear sense of when the information collected about an individual user would transform into "knowledge" that the user is a child, and that this uncertainty would likely lead operators of general-interest sites to collect more information about every user in order to ascertain their users' ages (or seek to exclude older minors), rather than risk inadvertently violating COPPA). *See also* Comments of TechAmerica at 4; MPAA 2010 Comments at 11 ("Adoption of [a constructive knowledge] standard … would require operators of general audience sites to investigate the ages of their site's visitors, necessitate age screening in sites that are not currently collecting age information and, as a result, increase data collection and reinforce undesirable activity by children.").

the Commission's conclusion that "[a]ctual knowledge is far more workable, and provides greater certainty, than other legal standards that might be applied to the universe of general-audience websites and online services."[17] As the FTC points out, consistent with the vast majority of commenters, changing the actual knowledge standard to a lesser standard, such as "constructive" or "implied" knowledge, would create enormous uncertainty for operators of general audience websites and services.[18] Although the actual knowledge standard may have some limitations, MPAA agrees that it is the most appropriate standard to apply under the circumstances.

B. THE COMMISSION'S PROPOSAL TO EXPAND THE DEFINITION OF "PERSONAL INFORMATION" EXCEEDS ITS STATUTORY AUTHORITY

In the *Notice*, the Commission proposes for the first time to expand its definition of "personal information" under COPPA to include information that neither identifies individual children nor permits those individuals to be contacted.[19] As discussed below, this proposal exceeds both the purpose of COPPA and the scope of the Commission's authority to modify the statutory definition of personal information. In addition, the proposal in the *Notice* is not based on any identified harm to children that has arisen from the current definition of personal information under COPPA. Indeed, the Commission's proposed approach could needlessly restrict uses of non-personal data that would improve children's online experience and enhance their privacy. In connection with this proposal, the Commission would allow operators to collect and use screen names and persistent identifiers for purposes of internal operational activities "necessary to maintain the technical functioning of the Web site or online service."[20] In this

[17] *Notice* at 59806.

[18] *Id*.

[19] *Id*. at 59810-59813.

[20] *Id*. at 59830.

context, the Commission should clarify that internal operations include interactive, community-based features on websites and online services, including games and the sharing of comments on games, videos, message boards, and other content.

1. THE PROPOSALS ARE OVERBROAD AND EXCEED THE PURPOSE OF THE STATUTE

COPPA was enacted to serve important but quite specific purposes: to protect the online privacy and safety of children, especially in light of the threat of unwanted contact by predators and others who might put them at risk.[21] The means that Congress chose to advance this aim were equally specific: subject to limited exceptions, COPPA prevents commercial websites and online services from collecting and sharing children's personal information without the involvement and consent of their parents.[22] The use of anonymous screen names, user names, persistent identifiers and photographs, videos, and audio files that help operators to deliver appropriate content, or that otherwise facilitate online experiences that engage a child's imagination, does not implicate the concerns COPPA is intended to address. As the Commission correctly recognized when it adopted its COPPA Rule in 1999, and again when it retained the Rule without change in 2006, screen names, user names, and persistent identifiers that do not contain personal information as defined in COPPA, or that are not actually combined with such personal information by an operator, cannot properly be encumbered by legal requirements that are irrelevant to Congress's purpose.[23] Thus, the proposal to expand the definition of personal

---

[21] *See* 144 Cong. Rec. S11657 (daily ed. Oct. 7, 1998) (statement of Sen. Bryan) ("*Bryan Statement*"). Senator Richard Bryan (D-NV), along with Senators John McCain (R-NY) and Conrad Burns (R-MT), sponsored COPPA in the Senate in 1998.

[22] *Id.*

[23] *See Children's Online Privacy Protection Rule; Final Rule,* Statement of Basis and Purpose, 64 Fed. Reg. 59888, 59892-59893 (Nov. 3, 1999) ("*Statement of Basis and Purpose*"); *Children's Online Privacy Protection Rule,* Retention of Rule Without Modification, 71 Fed. Reg. 13247 (Mar. 15, 2006). Moreover, as Microsoft notes: "[S]ome limited collection of information collected online from children can actually enhance the privacy and safety of children online. Knowing a child's age and IP address or cookie ID, for example, can enable operators to prevent

information to cover anonymous screen names, user names, persistent identifiers and photographs, videos, and audio files is overly broad and inconsistent with the type of information that directly implicates children's privacy and properly falls under COPPA.

2. CONGRESS ONLY AUTHORIZED RESTRICTIONS ON THE USE OF INFORMATION THAT COULD BE USED TO CONTACT A CHILD (RESPONSE TO QUESTIONS 5, 6, 7 AND 8)[24]

Congress provided the Commission with only limited discretion to expand COPPA's definition of personal information, and the proposals in the *Notice* exceed that discretion. Specifically, in order to extend the definition to an identifier not expressly listed in the statute or associated by an operator with a listed identifier, the Commission must determine that the additional identifier, standing on its own, "permits the physical or online *contacting* of a *specific individual* …."[25] As Senator Bryan pointed out, 'contact' with an individual online "includes any … attempts to communicate directly with an individual."[26] Accordingly, information that cannot support an attempt to communicate directly with an identifiable person is outside the scope of COPPA's personal information category and, thus, should not be considered personal information under the COPPA Rule. As discussed further below, the Commission's proposed categories of information do not enable contact with a specific child and/or do not permit contact with a child outside a particular website, unless coupled with additional, individually identifiable information.

---

inappropriate advertisements, such as those for alcohol, from being displayed to children." Comments of Microsoft at 9.

[24] *Notice* at 59828.

[25] 15 U.S.C. § 6501(8)(F) (emphasis added). According to COPPA, "personal information" means "individually identifiable information about an individual collected online, including: (A) a first and last name; (B) a home or other physical address including street name and name of a city or town; (C) an email address; (D) a telephone number; (E) a Social Security number; (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph." *Id.*

[26] *Bryan Statement*, *supra* note 21.

Screen Names. As the Commission correctly recognizes, a screen name or user name that does not include an email address does not identify an individual and cannot be used to contact an individual.[27] The potential uses of screen names and user names cited in the *Notice* do not change this result. For example, services that permit the use of the same screen names on multiple sites ordinarily do not, as the *Notice* suggests, give multiple site operators the means to acquire individually identifiable information or to contact the users of those screen names. Similarly, the use of screen names, user names, and other anonymous credentials by MPAA members for cross-site login purposes does not involve the collection or sharing of individually identifiable information concerning the users of those credentials.

In fact, MPAA members affirmatively protect the online anonymity of children by discouraging the adoption of screen names and user names that can be used to identify an individual. For example, many MPAA members' sites instruct children to pick a user name that does not include a real name or email address. These practices are consistent with the Commission's guidance in its order adopting the COPPA Rule, and nothing in the record suggests that screen names or user names have been used to compromise children's privacy in the years since the Rule was adopted.[28] Moreover, expanding the definition of personal information to include screen names or user names would most likely increase costs for website operators, thereby reducing incentives to develop and improve educational, entertaining, and compelling websites and online services for children. Accordingly, the Commission should refrain from including screen names and user names in the category of personal information.

---

[27] *Notice* at 59810.

[28] In finding that operators have no affirmative duty to ascertain whether a screen name contains personal information, the Commission suggested that operators could warn children against using such information, as MPAA members have done. *See Statement of Basis and Purpose,* 64 Fed. Reg. at 59892, n. 3. ("Operators do not have a specific duty to investigate whether a screen name contains [personal] information. However, an operator could give children warnings about including such information in screen names, especially those that will be disclosed in a public forum such as a chat room.").

Persistent Identifiers. Like screen names and user names, persistent identifiers ordinarily do not permit the "physical or online contacting of a specific individual." Acquisition of an Internet Protocol ("IP") address, a customer number held in a cookie, a processor, device serial number, or a unique device identifier does not give the possessor of that information the means to contact users of the devices associated with those identifiers. The Commission correctly acknowledged this fact when it adopted, and later elected not to change, the present Rule, which treats persistent identifiers as personal information only when associated with one or more items of individually identifiable information. The *Notice* claims that subsequent developments compel a different conclusion, but the developments the Commission cites – such as the fact that handheld devices may have "one or more unique identifiers that can be used to persistently link a user across Web sites and mobile applications" – have to do only with available *uses* of persistent identifiers, not with their capacity to disclose personal information.[29] The use of persistent identifiers to acquire information about the uses of a device is not new and does not convert these anonymous device identifiers into personal information under the statute.[30]

Photographs, videos, and audio files. Finally, the references in the *Notice* to facial recognition technologies and information embedded in digital files (*i.e.*, metadata) do not support the inclusion of graphic and audio files in the personal information category.[31] For example, the *Notice* states that "facial recognition technology can be used to further identify persons depicted

[29] *Notice* at 59811-59812.

[30] Moreover, such concerns would be beyond the scope of COPPA and Congress's intent regarding COPPA, and trying to address them within the context of the COPPA framework could lead to unintended and negative consequences.

[31] *Notice* at 59813. The *Notice* also states that audio files may permit recognition of a child's voice, but does not say how this would be accomplished. *Id.* In the absence of any relevant record evidence, the Commission need not specifically include that supports the inclusion of audio files in the definition of personal information.

in photos."[32] However, facial recognition technologies are still at a nascent stage of development. It is possible that website operators will be able to deploy such technologies in a manner that protects children, such as by stripping any geolocation metadata from images before posting. Such precautions could eliminate privacy concerns. Thus, it would be premature to change the definition of personal information for COPPA purposes based on evolving facial recognition technologies, especially given that the Commission hosted a recent workshop and has just initiated a proceeding seeking public comment to gather information and consider the implications of these technologies.[33]

3. THE PROPOSED "INTERNAL OPERATIONS" EXEMPTION MUST BE BROAD ENOUGH TO ALLOW FOR MEANINGFUL ONLINE INTERACTIVITY

The *Notice* proposes to exclude screen names and user names from the personal information category when used "*for the internal operations* of the Web site or online service."[34] Similarly, the *Notice* proposes to exclude persistent identifiers from the personal information category when used to support "*the internal operations* of, or protect the security or integrity of, the Web site or online service."[35] Thus, even under an expanded definition of personal information, the Commission would not treat screen names, user names, or persistent identifiers as personal information when used for internal purposes. MPAA agrees that the use of screen names, user names, and persistent identifiers within a website should be allowed, provided the identifier does not facilitate the contacting of a specific child. To allow full website functionality, internal operations need to include interactive, online community features on

[32] *Id.* at 59813.

[33] The FTC hosted a workshop on Facial Recognition Technology on December 8, 2011. *See* Face Facts: A Forum on Facial Recognition Technology, FTC, *available at* http://www.ftc.gov/bcp/workshops/facefacts/ (last visited Dec. 21, 2011). *See also* FTC News Release, FTC Seeks Public Comments on Facial Recognition Technology (rel. Dec. 23, 2011), *available at* http://www.ftc.gov/opa/2011/12/facefacts.shtm.

[34] *Notice* at 59830 (emphasis added).

[35] *Id.* (emphasis added).

websites and online services, including gaming and the sharing of comments on game sites, videos, message boards, and other content. Any narrow reading of "internal operations" would be inconsistent with the statute and with Congress's intent that COPPA protections not compromise the benefits of the Internet.

C. THE COMMISSION SHOULD NOT ELIMINATE EMAIL PLUS AS A MECHANISM FOR OBTAINING VERIFIABLE PARENTAL CONSENT

The COPPA Rule establishes a "sliding scale" by which an operator, when collecting personal information for internal use only, may obtain verifiable consent from a parent through email plus an additional step.[36] This mechanism – obtaining parental consent via an email, coupled with an additional step – is known as "email plus." Email plus is simple to implement, easy for users to understand, and the least burdensome mechanism for parents to utilize. As the Commission notes, the approach enjoys "wide appeal among operators, who credit its simplicity."[37] As recently as 2006, the Commission extended use of this mechanism indefinitely, stating that the rule would not be modified until an acceptable electronic consent technology develops.[38] No such workable replacement has emerged,[39] nor does the record of comments compiled in 2010 support elimination of the rule.[40] The FTC should not eliminate email plus absent evidence of its failure and, even more importantly, without a workable plan to replace it.

---

[36] *See* 16 CFR § 312.5(b)(2). As the *Notice* states, such additional steps have included obtaining a postal address or telephone number from the parent and confirming consent by letter or telephone call, or sending a delayed confirmatory email. *Notice* at 59819.

[37] *Id.*

[38] *See id.*

[39] In June 2010, the Commission conducted a workshop ("2010 Workshop") to discuss possible changes to COPPA and spent a substantial amount of discussion time on email plus. While some participants asserted a lack of innovation in parental consent verification methods, no information was presented to demonstrate that email plus fails to accomplish the protections required by COPPA, and no alternative mechanisms were suggested.

[40] *See, e.g.*, Comments of the Digital Marketing Association at 10 (the sliding scale approach is a reasonable method of obtaining verifiable parental consent).

Any potential risk associated with email plus should be evaluated in light of the fact that email plus is used only where data is collected and used solely for internal purposes. Several of the commenters who argue against email plus appear to conflate their concerns about parental verification for the use of information for *external* purposes with the limited instances where email plus is utilized. These commenters do not distinguish between internal and external purposes, and fail to directly address the use of email plus for internal purposes.[41] At the 2010 Workshop, a panel discussed the usefulness of email plus. Even workshop participants who voiced disappointment in the lack of alternative methods developed by the industry conceded that email plus is "good enough for internal use."[42] One workshop participant noted that the use of email plus has facilitated parental involvement even for websites that are no longer collecting personal information.[43]

Moreover, the Commission's proposal vastly underestimates the burden that would be imposed on operators if email plus were eliminated. To obtain Office of Management and Budget ("OMB") approval for a new information collection under the Paperwork Reduction Act,[44] an agency must demonstrate that it has taken "every reasonable step to ensure that the proposed collection of information: (i) is the least burdensome necessary for the proper performance of the agency's functions to comply with legal requirements and achieve program

---

[41] *See, e.g.*, Comments of RelyID at 3; Comments of TRUSTe at 2-3.

[42] Remarks of Denise Tayloe, President, Privo, Inc., COPPA Workshop Transcript at 215-16; Privo Comments at 5 (suggesting that rather than eliminate email plus, the "plus" could be improved). *See also* Remarks of Martine Niejadlik, Senior Director, Risk & Business Intelligence, COPPA Workshop Transcript at 218-19 ("I think e-mail [sic] plus – I would agree, it is not as strong as some of the other methods, but when you sort of [mesh] practicality with safety, you know, it's really one of the only ones on the list that I think is a viable option for people.").

[43] Remarks of Shai Samet, Samet Privacy, LLC, COPPA Workshop Transcript at 222 ("I think e-mail [sic] plus has served a very beneficial purpose, and somewhat unrelated to what the law requires, what we're finding is that many of the kid friendly websites, especially those for younger kids, who have designed their chat functionalities so as not to allow personal information to go through, are still using e-mail [sic] plus to notify and get parents involved with the fact that their kids are using those sites.").

[44] 44 U.S.C. § 3101, *et seq*.

objectives; (ii) is not duplicative of information otherwise accessible to the agency; and (iii) has practical utility."[45] Retaining email plus is the only reasonable approach under these standards.

To be certain, prohibiting the use of email plus would necessitate more than the Commission's estimate of 60 hours to convert to a different method of parental verification.[46] Some operators would need to review and re-write their current privacy policies, which is a significant undertaking. Operators would also need to implement new methods to ensure parental consent, as well as more burdensome recordkeeping requirements, which would be ongoing. In addition to the increased paperwork burden, companies will need to secure additional resources to develop, plan, code, and test new procedures. Such changes are likely to impact current vendor agreements, which may trigger a new round of negotiations with business partners.

In sum, email plus has not outlived its usefulness.[47] While MPAA members support the continued development of new verification methods, the Commission should not discontinue the use of email plus as an acceptable method of verifiable parental consent.

D. OPERATORS SHOULD NOT BE RESPONSIBLE FOR ENSURING THIRD-PARTY COMPLIANCE

The Commission should not adopt its proposal to require each operator to "take reasonable measures to *ensure* that any third party to whom it releases children's personal information has in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information."[48] MPAA agrees that children's personal information

---

[45] 5 CFR § 1320.5(d)(1).

[46] *Notice* at 59827.

[47] Remarks of Parry Aftab, Director, Wired Safety and Wired Trust, Inc., COPPA Workshop Transcript at 219-20 (stating that "email plus is "a great way of getting parents out there to do something. Unless you can find a new way of doing this … e-mail [sic] plus works. Right now, it works… [I]t may not be time to kill it.")

[48] This discussion is in response to question 21 of the *Notice* at 59832; proposed 16 CFR § 312.8 (emphasis added).

deserves secure treatment, regardless of the entity that maintains that information; however, the proposed requirement that operators take measures sufficient to *ensure* compliance by vendors and other third parties might be misapplied to make operators the effective guarantors of those measures. As a practical matter, no business is in a position to exercise the same degree of control over another, independent business as it can exercise over its own operations. Further, such a rule could, in turn, diminish the incentives of third-party vendors to comply the Rule.

Instead of imposing this unrealistic supervisory obligation, MPAA urges the Commission to take the same approach it adopted in its Safeguards Rule implemented under the Gramm-Leach-Bliley Act.[49] The Safeguards Rule requires covered entities to take "reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue," and to require service providers "by contract to implement and maintain such safeguards."[50] Requirements of this kind, which mandate due diligence in vendor selection and negotiation of contractual commitments with vendors to secure personal data, are reasonable and achievable. Similar requirements should be adopted here.[51]

E. OPERATORS SHOULD BE PERMITTED A SINGLE POINT OF CONTACT

MPAA urges the Commission not to require that where a website or online service has multiple operators, the website or online service must provide contact information for all operators, rather than permitting the designation of a single operator as the contact point.[52] The

[49] 16 CFR § 314.4 (implementing the data security provisions of the Gramm-Leach-Bliley Financial Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999)).

[50] *Id.* at § 314.4(d).

[51] It may also be worth noting the data protection provisions of the Health Insurance Portability and Accountability Act, which require covered entities to obtain "reasonable assurances from the person to whom [protected health information] is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person." 45 CFR § 164.504, implementing the data security provisions of the Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[52] *Notice* at 59815.

Commission suggests that providing multiple points of contact "will aid parents in finding the appropriate party to whom to direct any inquiry."[53] However, in the experience of the MPAA member companies, by designating a single point of contact, multiple site operators can ensure that parents' inquiries are directed to the appropriate operator for resolution and that all operators are apprised of the concerns expressed by parents. Foreclosing this option will reduce the efficiency of website operations and is likely to confuse parents more than it aids them. Moreover, a single point of contact allows for better control of the process and increases consistency in an operator's responses to any concerns. In the absence of any information in the record suggesting that designation of single points of contact prevented the resolution of parental inquiries, there is no basis to amend the Rule to require multiple points of contact.

F. THERE IS NO NEED TO AMEND THE TOTALITY OF THE CIRCUMSTANCES TEST TO INCLUDE NEW SUBJECTIVE CRITERIA

The Commission's present method of determining whether a website or online service is directed toward children reflects a "totality of the circumstances" approach that is workable and should be retained in its current form.[54] Using this approach, the Commission examines all elements of a website's content that might disclose the operator's intent to appeal to children under the age of 13.[55] The definition includes a non-exclusive list of factors that the Commission will take into account, but states that "the Commission will look at the overall character of the site – and not just the presence or absence of one or more factors – in determining whether a website is directed to children."[56] As the *Notice* explains, the test "provides sufficient coverage and clarity to enable websites to comply with COPPA, and the

[53] *Id.*

[54] *Id.* at 59814.

[55] *Statement of Basis and Purpose,* 64 Fed. Reg. at 59893, 59912-59913.

[56] *Id.* at 59893.

Commission and its state partners to enforce COPPA."[57] Thus, the Commission correctly concludes that adoption of a *per se* test, such as audience demographics showing that 20 percent or more of a site's visitors are under the age of 13, would prove less reliable than the Commission's present approach.[58]

For the same reasons, the Commission need not modify the definition to include musical content or celebrities that appeal to children. These changes would muddy the waters and add uncertainty to a test that the Commission has found, in its current form, provides clarity to industry and regulators alike. For example, the proposed addition of "the presence of child celebrities or celebrities who appeal to children" to the definition's list of non-exclusive factors, would make the definition less reliable as a means of identifying sites directed to children.[59] The age of a celebrity does not necessarily correlate to the age of the celebrity's fan base, and celebrities who appeal to children might have equal or greater appeal to teens or adults. Reliance on this added factor might therefore produce results that are less accurate than a "totality of the circumstances" analysis that does not include this factor.

Similarly, although the term "audio content" in the existing rule could apply to music on a website, specifically adding music to the factors to be considered would overstate the value of such information in determining whether a site is directed to children. As in the case of celebrities, with some minor exceptions, the fan base for a particular musician or band cannot easily be classified as children-only. Accordingly, reliance on music content on websites likely would not produce consistently reliable results in determining whether any specific website is directed at children. MPAA thus urges the Commission to retain its present, workable definition

[57] *Notice* at 59814.

[58] *Id.* ("[S]uch [demographic] data is neither available for all Web sites and online services, nor is it sufficiently reliable, to adopt it as a *per se* legal standard.").

[59] *Id.*

of "website or online service directed to children" without the added factors of music content or celebrities' ages or presumed appeal to children.

IV. CONCLUSION

Even with dynamic changes in online content and service offerings since COPPA was enacted, the existing COPPA Rule continues to provide a workable regulatory framework that protects and safeguards children. There is no need for amendment of the Rule that could curtail the benefits of the Internet without any corresponding benefit to child safety. The MPAA and its members fully support the Commission's efforts to implement and enforce Congress's mandate to protect children's privacy, and the MPAA looks forward to continuing to work with the Commission in this regard.

Respectfully submitted,

MOTION PICTURE
ASSOCIATION OF AMERICA, INC.

By: *_/s/ Linda Kinney_*

Michael O'Leary
Senior EVP, Government Relations
Linda Kinney
Vice President, Regulatory Affairs
1600 Eye Street, NW
Washington, DC 20006
(202) 378-9139

December 23, 2011