Before the

FEDERAL TRADE COMMISSION

IN THE MATTER OF COPPA RULE REVIEW

Project No: P-104503

COMMENTS OF THE PROMOTION MARKETING ASSOCIATION, INC.

COMMENTS OF:

Promotion Marketing Association, Inc.

Edward M. Kabak
Chief Legal Officer

Counsel of Record:

Alan L. Friel
EDWARDS WILDMAN PALMER, LLP

Marc S. Roth
MANATT, PHELPS & PHILLIPS, LLP

The Promotion Marketing Association, Inc. ("PMA") respectfully submits these Comments in response to the request by the Federal Trade Commission ("FTC" or "Commission") in connection with its notice of proposed rulemaking for revisions to its implementation of the Children's Online Privacy Protection Act ("COPPA" or the "Act"), 15 U.S.C. §§ 6501-06, through the Children's Online Privacy Protection Rule ("COPPA Rule") 16 C.F.R. § 312 (1999). 76 FR Vol. 76, No. 187, 59804-59833 (September 27, 2011) ("NPR"), as revised by its Supplemental Notice of Proposed Rulemaking, 77 FR Vol. 77 No. 151, 46643-46653 (August 1, 2012) on the same proposed rulemaking ("SNPR").[1] In addition, the PMA comments on a Request to Investigate McDonalds Corp., *et al* for COPPA Violations in Conjunction with Viral Marketing to Children combined with Comments on the SNPR filed by the Center for Digital Democracy ("CDD").

I. The PMA

Established in 1911, the PMA is the leading not-for-profit trade organization and resource for research, education and collaboration for marketing professionals. Representing the over $1 trillion integrated marketing industry, the organization is comprised of Fortune 500 companies, top marketing agencies, law firms, retailers, service providers and academia, representing thousands of brands worldwide. Championing the highest standards of excellence and recognition in the promotion and integrated marketing industry globally, the PMA's objective is to foster a better understanding of promotion and integrated marketing and its role in the overall marketing process.

The PMA recognizes the importance of the underlying intent of COPPA: to provide reasonable and practical safeguards to foster efforts to protect young children online and give parents reasonable tools to help them guide their children's online activities. The PMA believes that COPPA and the current COPPA Rule establish an appropriate, and now well established scheme that strikes a proper balance between protecting children and recognizing the practicalities and challenges of operating within an online environment and the importance and benefits of the Internet and e-commerce to the consumers of the United States, including children. However, as set forth below, the PMA respectfully submits that many of the Commission's proposed changes are ill advised, not supported by any evidence of harm that is in need of redress and would create an undue burden on industry that will likely result in reduced online offerings made available to children.

II. SUMMARY

As more fully set forth below, the PMA respectfully submits that the FTC should:

- revise how it proposes to define and treat "operators" and "website or online service directed to children",

[1] Page and footnote cites to the SNPR and NPR will be to the SNPR and NPR as published by the FTC, not to the Federal Register version.

- permit mixed audience sites to age screen users and apply the COPPA-mandated protections only to those who self-identify as children under 13, as opposed to all users of the site, However, it should not force that obligation on general audience sites that are not directed to children if they have "child-oriented content appealing to a mixed audience, where children under 13 are likely to be an over-represented group."

- modify its proposal to treat persistent identifiers used to recognize a user over time or across sites as personal information,
- better clarify that the "support for internal operations" exception explicitly excludes from coverage the use of persistent identifiers for internal activities,
- expand the types of activities to be included in the "support for internal operations" exception, and
- modify its proposal to treat user names and screen names as personal information only if that identifier is associated with functionality that permits the person to be contacted online.

In addition, for the reasons previously set forth in our Comments to the NPR, attached hereto as Exhibit A, the PMA (i) continues to urge retention of E-Mail Plus and the one-time use exceptions for prize fulfillment for promotions and for send-to-friend e-card promotions; (ii) supports the proposed additional exception to verified parental consent requirements; (iii) objects to the proposal to require an online notice to list all operators rather than a single responsible operator; and (iv) objects to the proposal to include in the definition of Personal Information persistent identifiers, geo-location data, screen names, photos, videos and audio files, date of birth, gender and/or ZIP code.

III. PMA'S COMMENTS TO THE SNPR

A. THE FTC should revise how it now proposes to define and treat "operator" and "website or online service directed to children", in particular with respect to when an operator of a site or service directed to children should be deemed to be responsible for the data collection practices of third parties on or via its site or service, such as ad networks, third party social networking services and downloadable software providers.

Currently, an operator of a site or service directed to children under 13 that both collects the information, and also maintains ownership, control and access to it, would be responsible for COPPA compliance (such as obtaining verified parental consent ("VPC") before collecting personal information). Facilitating a third party's collection is not currently covered. The FTC proposes to revise the definitions to hold both the third party collecting personal information and the site operator allowing such collection by third parties responsible, but with different standards of care.

Children's site operators are, under the SNPR, proposed to be required to ensure that advertisers, ad networks, ad exchanges, software kit and patch providers, widget and application publishers and others that interact with their site or service are not collecting personal information from children under 13 absent VPC. A failure would appear to result in strict liability for these operators, regardless of knowledge.

Conversely, those third parties that collect personal information on sites or services operated by others are under the SNPR proposed to also be responsible for ensuring COPPA compliance, with respect to their activities on children's sites, or portions of sites directed to children, but only if they "know or have reason to know" that they are interacting with a site or service directed to children. This is not a strict liability standard, but rather applies a willful blindness standard. While the FTC says in its SNPR that this will not impose a duty to investigate or monitor what sites and services these third parties' services are integrated into, "they will not be free to ignore credible information brought to their attention" and that the change "requires a person to draw a reasonable inference from the information he does have."

The PMA believes that in both cases the approach and standards are too strict.

For children's websites (or with respect to self-identified children on mixed use sites, discussed in Section III.C, below), we propose that the operators only be responsible for third parties' activities related to their site if they: (i) have given the party direct consent to interact with the site and failed to require them to comply with COPPA; (ii) affirmatively act to implement the third party's technology into the site and failed to require the third party to comply with COPPA; or (iii) "know or have reason to know" that a third party is interacting with the site in a way that fails to comply with COPPA. The ability to operate within the online and mobile ecosystem has become too complex with too many third parties interacting with sites and apps, sometimes without the knowledge or consent of the operator, to hold the operator responsible absent the operator having acting directly to involve the third party and failed to require it to comply with COPPA. That is all that is reasonable to ask of operators and a greater burden is likely to result in sites that lack the functionality of today's sites and apps. Further, it is not reasonable to expect operators, particularly small businesses, to undertake to ensure those third parties act in compliance with law, beyond requiring them to give the third parties they authorize or integrate, notice of COPPA obligations and to take action when the operator knows or has reason to know they are not complying. This is particularly true since the operator typically has no way of monitoring or knowing what the third party is or is not in fact doing. In the end, the company responsible for collecting and using children's information should be responsible for complying with COPPA.

Related to these issues is the FTC's proposal in its NPR that operators list the contact information for all third parties that collect personal information. This should also be subject to the "knows or has reason to know" standard.

Finally, the FTC should clarify that use of third party tracking technologies to the extent used for internal purposes as discussed more fully below in Section III.B, should not require VPC.

As for third parties that collect personal information on sites or services operated by others, we recommend an actual knowledge standard, the standard under the COPPA Rule that is applied to general audience web sites that are not directed to children, but on which children might be present. Under our proposal above, if operators are providing the notice we recommend be required, these parties will have actual knowledge. The "has reason to know" standard is too amorphous for third party technology providers and service agents who may be

integrated by operators when the burden of notice can be placed on the operators, who are best able to know if their sites are subject to VPC obligations.

B. The FTC should permit mixed audience sites to age screen users and apply the COPPA-mandated protections only to those visitors who self-identify as being under 13, as opposed to all users of the site. However, it should not force that obligation on general audience sites that are not directed to children if they have "child-oriented content appealing to a mixed audience, where children under 13 are likely to be an over-represented group."

The current COPPA Rule requires operators of sites, or portions of sites directed to children to treat all users as children. A significant benefit of the new proposal is that if a mixed audience site operator, or presumably a third party integrated into such a site such as a social media plug-in or an online behavioral ad network or exchange, age screens its users it can treat those that self-identify as 13 or over as adults. Those older users could then be offered chat and social networking services, and their behavior could be tracked to serve them with ads based on their online behavior. This will promote an increase in content for families and children, in part by giving family-friendly sites more flexibility to provide more robust activities and personalized ads for users 13 and over.

The FTC invites comments on how this could be practically implemented, and one seemingly obvious issue is how to deal with multiple users of a family computer. Dropping a cookie on the computer or blocking its IP address to designate a child, would also result in other family members being similarly treated. A solution could be individual users accounts for site users, but many sites are open to unregistered users and for those, identification issues will need to be solved. However, if the proposed rules for mixed-use sites are optional for the sites that seek such treatment, the practical implementation challenges are less concerning to us than if the proposed rulemaking proceeds as is.

As we read the proposal, a general audience site that does not target children but has content that might attract them and has a greater percentage of users under 13 than is present in the general population, would be required to act as a mixed-audience site and undertake the challenging implementation of age screening and treating users identifying as under 13 or 13 or over differently. In its NPR, the FTC expressly rejected dilution of the actual knowledge standard for general audience sites and found user age demographic statistics to be inherently untrustworthy. NPR, Section III, pp. 9 – 14 and Section V.A.7, pp 45-46 ("The Commission's experience with online audience demographic data … shows that such data is neither available for all websites and online services, nor is it sufficiently reliable, to adopt a per se legal standard.") Why now then does the FTC seek to change this position? To do so would result in operators of sites that target teens and college students (e.g., apparel manufactures and retailers, broadcast networks, pop music labels) to have to "ferret through a host of circumstantial information" to determine if they are required to age gate merely because children aspiring up and in a proportion greater than in the general population may visit their site notwithstanding the absence of any efforts to attract them. (See FTC express rejection of such an obligation at NPR p. 13). Furthermore, as the FTC correctly noted in its NPR, such a change would require Congress to change the actual knowledge standard in COPPA, and thus is beyond the FTC's rule making authority (unless it is something an operator can opt into).

C. The FTC should (i) modify its proposal to treat persistent identifiers (e.g., IP address, mobile device identifier, an identifier associating a computer with a cookie) used to recognize a user over time or across sites as personal information, (ii) better clarify that the "support for internal operations" exception explicitly excludes from coverage the use of persistent identifiers for internal activities, (iii) expand such activities beyond what is now proposed to be specifically identified as site maintenance and analysis, performing network communications, authenticating users, setting and maintaining user preferences, serving contextual advertisements (but not behaviorally targeted ads), protecting against fraud, and responding to certain requests of users, so long as the information is not used to contact a specific individual.

The FTC's original proposed changes were, it stated, intended to require VPC for using persistent identifiers "for purposes such as amassing data on a child's online activities or behaviorally targeting advertising to the child". As we noted in our original comments at Exhibit A, it was not clear what would amount to the prohibited amassing of data, as opposed to permitted internal uses. The SNPR proposed changes seem to seek to clarify what types of use of persistent identifiers are and are not permitted when they are collected on a site directed to children or knowingly from a child. The PMA welcomes the further guidance, but believes that in doing so, the FTC has not gone far enough to permit the reasonable operations of sites and services that rely on the use of persistent identifiers for internal purposes. As previously noted, persistent identifiers *identify devices* not individuals and the primary purpose of COPPA – to prevent the contacting of children absent parental consent – could be achieved by treating persistent identifiers as personal information only if they are used to contact a child. In other words, *regulate the use* not collection of persistent identifies. The FTC noted numerous comments urging this approach, but has chosen to disregard them. Also, the Commission failed to respond to comments pointing out that it attempts to draw a line between "contextual" and "behavioral" advertising, with identifiers used for "contextual" advertising being permissible while identifiers for "behavioral" advertising requiring prior verified parental consent, but it fails to define the terms. This seems like a distinction without a difference, as all "contextual" ads depend upon some action taken by the computer user (*e.g.*, entering a search string, viewing certain content, engaging in certain activities) - this sounds an awful lot like "behavioral" advertising and the FTC still does not explain how it interprets the difference between the terms.

Accordingly, the FTC should further expand the definition of support for internal operations to explain where it draws the line between contextual and behavioral advertising, to permit use of identifiers for coordinating operations by a single operator over multiple platforms and between affiliated websites and online services (an approach the FTC appears now willing to accept for screen names as discussed below) and to clarify that the list of permitted internal uses are examples and not an exhaustive list and that any use other than to contact an individual with a direct third party ad or message, is an internal operations purpose.

D. The FTC should modify its proposal to treat user names and screen names as personal information that requires VPC to collect only if that identifier is associated with functionality that permits the person to be contacted online (i.e., it functions as an instant message or e-mail address).

The PMA supports this proposed revision. This would permit operators who use user names for certain internal administrative purposes and for operators of a service accessible by multiple platforms and devices and operators of a family of sites or applications to do so without VPC, which is consistent with the intent and purpose of COPPA. As noted above in Section III.C, the Commission should take a similar approach to persistent identifiers. At the same time, we urge the FTC to clarify that an identifier that is not capable of permitting a person to be contacted online should be declared an exception under internal operations.

IV. PMA'S COMMENTS TO THE CDD'S COMMENTS AND REQUEST

The CDD argues in its Comments and Request that (1) send-to-friend e-mail campaigns are harmful and should be prohibited by COPPA absent VPC of both the recipient and the sender and COPPA FAQ #44 should be rescinded; (2) associating third party cookies that track persistent identifiers and other information not currently considered to be Personal Information in connection with send-to-friend e-mails should be prohibited by COPPA absent VPC; and (3) photos should be treated as Personal Information under COPPA.

A. Send-to-friend e-mail campaigns, even where marketing messages are included, should fall within the one-time use exception under COPPA and should continue to be permitted without VPC.

We addressed the one time use exception for e-cards and contest / sweepstakes fulfillment in our prior comments. Exhibit A at pp 4 - 6. Under the current COPPA Rule, as explained by the FTC in its FAQs, such activities are permitted without VPC. They should continue to be so excepted and as our prior comments illustrate, some minor language changes in the NPR's proposal need to be revised to make this clear. The CDD's objections appear to primarily address the substance of promotional content that might be included in viral e-cards and they argue children cannot easily distinguish between advertising and other content. This position is insufficient to justify terminating the one time use exception that enables operators to facilitate single use viral e-cards from one user to another. The issue of labeling of promotional content to address such concerns is not within the scope of COPPA. Rather, the CARU Self-Regulatory Guidelines police this issue. Further, requiring age screening of recipients of viral e-cards prior to collection of such information from a sender, as the CDD seems to promote, is not practical, and thus such a change would preclude send-to-friend tools outright (at least for sites or services directed at children).

Further, many websites include "refer-a-friend" or "share" options to allow users to identify and forward items of interest like online games to friends via email. Allegations that these functionalities are illegal viral marketing campaigns violate COPPA are simply without merit. These activities fully comply with existing COPPA requirements and are consistent with widespread industry best practices for child-directed websites as set forth by the Commission in its FAQs. In fact, many companies refer to and rely upon FAQ 44, which interprets the "one-

time contact exception"[2] as applied to e-cards and refer-a-friend features, when designing share and refer -a-friend features.

B. Associating third party cookies that track persistent identifiers and other information not currently considered to be Personal Information in connection with send-to-friend e-mails should (i) be treated as permitted internal purposes exempt from VPC with respect to use by the operator of the send-to-friend e-card; and (ii) as to the use thereof by the third party, should be treated as suggested in Section III.A above.

The CDD's objections to the use of cookies in association with send-to-friend e-cards illustrates the issues raised above in Sections III(A) and (III)(C) regarding both the responsibility for third party collection activities and the scope of internal uses that should be permitted for persistent identifiers. It should be a permitted internal use for an e-card operator to track functionality and other analytics related to the cards. It would be reasonable for operators of e-card services directed at children to have to give notice to any third party technology services it uses in this regard that the e-card service is directed at children and thus the third party needs to restrict its related activities to being in compliance with COPPA. However, it is unreasonable to impose strict liability on that operator for the third party's failure to comply, something it cannot practically ensure.

C. Photos and other user-generated content should not be treated *per se* as Personal Information under COPPA.

The CDD objects to collection and display of children's photos by operators and marketers, even where there is no additional information that might reasonably enable a viewer to identify and contact the children. For the reasons previously raised in our original comments (see Exhibit A p. 12), a *per se* rule treating all photos as Personal Information will not prevent the harm COPPA is meant to guard against – requiring VPC before information that enables personal contact is collected. The PMA does not object to treating photos that include information that could enable contact to be treated as Personal Information as is the current approach (e.g., the image includes a phone number or other contact information). However, operators that desire to allow children to provide user generated content (UGC), such as photos, should have the ability to screen such content to weed out images that include contact information. Treating images, photos, audio files and other user generated content as Personal Information, without more, simply deprives children of the ability to engage in UGC activities and is likely to drive them to general audience sites where they will misrepresent their age to gain access. This is far more dangerous than permitting regulated UGC activities on children's sites. A better approach would be for the FTC to require only reasonable efforts to weed out all or virtually all contact information from such types of content, as it has done with site and

[2] 15 U.S.C. § 6502(b)(2)(A). Contrary to the suggestion in the complaint that companies' share features cannot rely upon the parental consent exemption in Section 312.5(c)(2) because it does not seek verifiable consent from the recipient's parents, FAQ 44 clearly anticipates that such features involve the provision of the recipient's email address and that only implementations "providing the opportunity to reveal any personally identifiable information (PII) ***other than the recipient's email address*** requires you to obtain heightened verifiable consent from the ***sender's*** parent." *Id*. (emphasis added).

service activities generally in proposing to end the 100% deletion standard. NPR at p.21. As the Commission stated: "Unfortunately, websites that provide children with only limited communications options often fail to capture their imaginations for very long." Id.

V. CONCLUSION

The PMA supports reasonable efforts to protect children and maintain parent's reasonable expectations of privacy for their children using ever-evolving online media and technology. PMA appreciates the FTC's review of the COPPA Rule and its efforts to keep it relevant. Our members are, however, concerned that some of the proposals and suggestions in the NPR and SNPR, and the FTC's dismissal of prior industry comments in its rulemaking process may have unintended and detrimental effects and in some instances exceed Congress's intention for COPPA.

Further as outlined in our prior comments at Exhibit A, some of the previously proposed changes, such as elimination of E-Mail Plus, are merely to promote innovation rather than to address any harm, and will result in additional costs for industry that will reduce content available to children. Other changes may too have unintended effects, such as the proposed language change to the one-time use exception, and as such, PMA seeks clarification that the one-time use exception remains available for contacting parents to get an address to send a prize and for facilitating e-cards sent by children. PMA is also concerned about treatment of additional categories of information as *per se* Personal Information when they cannot in many instances enable personal identification or contact and we find the carve outs for internal uses to be too restrictive as written and in need of further expansion and clarification such as has been attempted with persistent identifiers. If any material changes are implemented, we urge a prospective implementation (i.e., "grandfather" existing users), and sufficient time to develop new site tools and activities before the new rules go into effect. We trust that the Commission will take these comments and concerns into account in finalizing the COPPA Rule revisions.

Exhibit A to PMA filing under Project No: P-104503: namely, earlier comments made and filed December, 2011

Before the

FEDERAL TRADE COMMISSION

IN THE MATTER OF COPPA RULE REVIEW

Project No: P-104503

COMMENTS OF THE PROMOTION MARKETING ASSOCIATION, INC.

COMMENTS OF:

Promotion Marketing Association, Inc.

Edward M. Kabak
Chief Legal Officer

Counsel of Record:

Alan L. Friel
Jesse Brody
EDWARDS WILDMAN PALMER, LLP

Marc S. Roth
La Toya Sutton
MANATT, PHELPS & PHILLIPS, LLP

John Feldman
REED SMITH, LLP

Justine Gottshall
INFOLAW GROUP

The Promotion Marketing Association, Inc. ("PMA") respectfully submits these Comments in response to the request by the Federal Trade Commission ("FTC" or "Commission") in connection with its notice of proposed rulemaking for revisions to its implementation of the Children's Online Privacy Protection Act ("COPPA" or the "Act"), 15 U.S.C. §§ 6501-06, through the Children's Online Privacy Protection Rule ("COPPA Rule") 16 C.F.R. § 312 (1999). 76 FR Vol. 76, No. 187, 59804-59833 (September 27, 2011) ("NPR")[3].

Established in 1911, the PMA is the leading not-for-profit trade organization and resource for research, education and collaboration for marketing professionals. Representing the over $1 trillion integrated marketing industry, the organization is comprised of Fortune 500 companies, top marketing agencies, law firms, retailers, service providers and academia, representing thousands of brands worldwide. Championing the highest standards of excellence and recognition in the promotion and integrated marketing industry globally, the PMA's objective is to foster a better understanding of promotion and integrated marketing and its role in the overall marketing process.

The PMA recognizes the importance of the underlying intent of COPPA: to provide reasonable and practical safeguards to foster efforts to protect young children online and give parents reasonable tools to help them guide their children's online activities. The PMA believes that COPPA and the current COPPA Rule establish an appropriate, and now well established scheme that strikes a proper balance between protecting children and recognizing the practicalities and challenges of operating within an online environment and the importance and benefits of the Internet and e-commerce to the consumers of the United States, including children. However, as set forth below, the PMA respectfully submits that many of the Commission's proposed changes are ill conceived, not supported by any evidence of harm that is in need of redress and would create an undue burden on industry that will likely result in reduced online offerings made available to children.

As more fully set forth below, the PMA urges retention of E-Mail Plus and the one-time use exceptions for prize fulfillment for promotions and for send-to-friend e-card promotions; supports the proposed additional exception to verified parental consent requirements; objects to the proposal to require an online notice to list all operators rather than a single responsible operator; and objects to the proposal to include in the definition of Personal Information persistent identifiers, geo-location data, screen names, photos, videos and audio files, date of birth, gender and/or ZIP code.

1. Elimination of E-Mail Plus - The FTC proposes to eliminate the E-Mail Plus / sliding scale method of parental verification for collection of Personal Information for internal uses (i.e., other than disclosure to third parties), currently at Section 312.5(b)(2). The PMA objects. First, the Commission acknowledges that E-Mail Plus has been widely adopted and is supported by industry. Indeed, sites and business models have been built around it. The Commission does not point to, or even suggest, a single incident of harm arising out of the use of the method. In short, it works and it does not put children at risk. A change without a harm to mitigate is not reasonable, particularly where it will result in an expensive reworking of sites and business methods.

[3] Page and footnote cites to the NPR will be to the NPR as published by the FTC, not to the Federal Register version.

The Act, which governs the Commission's rule making authority in implementing the COPPA Rule, provides for "*any reasonable effort* (taking into consideration available technology) … to ensure that a parent of a child receives notice of the operator's Personal Information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of Personal Information and the subsequent use of that information before that information is collected from the child." 15 U.S.C. § 6501(9) (emphasis added). Currently, E-Mail Plus is permitted for certain internal uses of information not shared with third parties or subject to public disclosure. 16 C.F.R. § 312.5(b)(2). E-Mail Plus remains a reasonable method of notice and verification where the operator is not going to disclose Personal Information to third parties nor will the operator make it publicly available. When the uses are solely internal, the potential for third parties to contact children without their parent's knowledge or consent, the precise goal that COPPA is intended to address, is not present. It was for this reason that the sliding scale for the requisite level of verification was and remains reasonable.

E-Mail Plus weighs practicality and safety and recognizes that e-mail is the primary way we communicate today and gives parents a tool they can easily use. At the same time, the "plus" aspect provides a reasonable safeguard that is less vulnerable to manipulation or circumvention than the neutral age gating that is used to exclude children from restricted content and activities and as reliable as some forms of verified parental consent, such as returning faxed and scanned parental content forms, both of which may be easily faked by children with basic computer operations skills. E-Mail Plus allows a marketer or operator to send an e-mail to the parent giving notice of the information collection "coupled with additional steps to provide assurances that the person providing the consent is the parent." 16 C.F.R. § 312.5(b)(2). The current COPPA Rule further provides: "Such additional steps include sending a confirmatory e-mail to the parent following receipt of consent; or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. Operators that use such methods must provide notice that the parent can revoke consent given in response to the earlier e-mail." *Id*. While merely sending a confirmatory e-mail to the same e-mail address does not help if the e-mail the child submitted as the parent's was not in fact that of a parent, other steps to obtain reasonable assurance that a parent got the notice, such as requiring an e-mail response from the parent that includes information that would provide reasonable assurance that the correspondent was an adult (such as could be done through responses to questions), a notice by mail addressed to "the parents of [Child]" or a follow up phone call *are* reasonable methods of assurance. As such, these and other reasonable steps that are less stringent than what the Commission approves as forms of verified consent should remain available for collection and use of Personal Information other than "disclosures" defined under 16 C.F.R. § 312.2.

In its commentary to the proposal to eliminate E-Mail Plus, the Commission does not identify a single incident of harm or potential harm caused by, or a single parental complaint concerning E-Mail Plus, and acknowledges that web site operators and marketers have come to rely on it and are satisfied with it. Rather, the FTC proposes to eliminate it "in the interest of spurring innovation." That, we respectfully submit, is not a legitimate purpose, it is not likely a purpose the Act mandates, and it is contrary to the fundamental underpinnings of the Commission's Section 5 authority, which is based on protecting consumers from harm. Further, the Commission acknowledges that in adopting E-Mail Plus as a reasonable method, it "was persuaded by commentators' views that internal uses of information … present[] less risk than external disclosures…."[4] The Commission provides no basis of support for now concluding otherwise. Internal uses still present a far lower risk of harm (if any at all), and thus a sliding scale of verification remains a reasonable method of evaluating the sufficiency of notice and consent. Furthermore, the Commission is acting contrary to its own standard for "reasonableness" that it applies in proposing to abandon the 100% deletion standard in connection with social media platforms for establishing when Personal Information is "collected" in lieu of "a 'reasonable methods' standard whereby operators who employ technologies reasonably designed to capture all or virtually all Personal Information inputted by children should not be deemed to have 'collected' Personal Information."[5] There, the Commission called for "a broad standard of reasonableness".[6] PMA respectfully suggests that the Commission apply the same standard with respect to E-Mail Plus for purposes of internal uses.

Eliminating E-Mail Plus will make it much more difficult for sweepstakes and contest operators to obtain reasonable assurances that parents do not object to the collection of a mailing address necessary to notify a child that she has won. The proposed changes to the Section 312.5(c)(2) one-time use exception discussed in point 2 below, exacerbate this problem. The time, effort and cost of undertaking a more complex method of verified parental consent will result in more expense for promotions to children and, as such, they will certainly be used less frequently as a result. This reduces opportunities for children and burdens industry when there is no indication of any harm being offset by these changes.

The same is true for our members that offer online content to children. By eliminating this option for collection where disclosure will not occur, especially given the proposed expansion of Personal Information to include screen name, photos and other new categories of information (discussed below), many of our members will be forced to eliminate current online offerings for children (unless the new rules are applied only prospectively and current users are grandfathered), and to reduce new offerings, due to the increased cost that verification requires (e.g., increased staff, more time intensive efforts, investments in new technology, etc.). If the Commission values free, fun, harmless entertainment and educational content for children, it should not make it more burdensome for companies that do not disclose their users' Personal Information to offer that content.

[4] NPR at p. 65, fn. 147 (citing 1999 Statement of Basis and Purpose, 64 FR 59888 - 59901).
[5] *Id.* at p. 21.
[6] *Id.* at p. 21, fn. 53.

2. Elimination of One-Time Exception for Prize Fulfillment and Send-to-Friend. Changes to 312.5(c)(2), now 312.5(c)(3), the one-time use verification exception and notice requirement, appears to eliminate the ability for operators to use the exception to the verified parental consent requirement for promotion prize fulfillment and send-to-friend e-Mails. The PMA respectfully objects.

The proposed revisions in the NPR could be read as calling into question the FTC's current position that the one-time use exception of Section 312.5(c)(2) permits collection of online contact information to contact a parent to obtain a mailing address to send a prize that a child has won or to facilitate sending an e-card initiated by a child, in both cases where no other use of that information is used. This is due to a very slight wording change. The PMA assumes that the FTC did not intend to change its position on these uses as a result of the wording change and seeks clarification that these uses remain under the one-time use exception.

Operators of sweepstakes, contests and promotions rely on the one-time use exception to efficiently obtain a mailing address from a parent to send premiums or prizes to children. In its October 7, 2008 FAQs about the COPPA Rule (the "FAQ"), the Commission specifically approved of this approach:

> "42. I want to have a contest on my site. Can I use the one-time contact exception to parental consent?
>
> ….If you wish to collect any information from children online beyond an email address in connection with contest entries – such as collecting a winner's home address to mail a prize – you must provide parents with direct notice and affirmatively obtain prior parental consent, as you would for other types of personal information collection beyond an email address. <u>If you do need to obtain a mailing address and wish to stay within the one-time exception, you may ask the child to provide his parent's email address so that the parent may be notified if the child wins the contest. In the prize notification email, you can ask the parent to provide the home mailing address to ship the prize, or invite the parent to call a telephone number to provide the mailing information.</u>" [emphasis added]

The key provision of the COPPA Rule was Section 312.5(c)(2), which is now proposed to be Section 312.5(c)(3). Old Section 312.5(c)(2) provided the exception "where the operator collects OCI [online contact information] from a child for the sole purpose of responding directly on a one-time basis to a specific request from the child, and where such info is not used to recontact the child and is deleted by the operator from its records." (Emphasis added.) Proposed new Section 312.5(c)(3) would provide the exception "where the sole purpose of collecting a child's OCI [where (c)(2) permits collecting the parent's] is to respond directly on a one-time basis, is a specific request from the child, and where such info is not used to recontact the child or for any other purpose, is not disclosed, and is deleted by the operator from its records after responding to the child's request." (Emphasis added.) A promotions operator needs the parent's e-mail, not the child's, to contact the parent and get the mailing address for prize fulfillment to stay within the one-time use exception and avoid having to obtain verified parental consent. The changed language prevents this, and thus FAQ #42 seems to lose its basis of support. Furthermore, the current scheme furthers the maxim that operators should only collect the information necessary to enable children to participate in an activity. If 100,000 children enter a contest or sweepstakes, but only five will win prizes that will be mailed to them, it need not collect physical addresses from all (and thus require all to obtain verified parental consent as a condition of entering). And, waiting until winners are selected to inform them that they must obtain verified parental consent to receive the prize is likely to result in an inability to obtain such consent from some resulting in prizes going unawarded (a regulatory problem in some jurisdictions) or a more complex selection, awarding and fulfillment method requiring the need for selection of runners up. In either event, the same additional costs discussed above will apply and we have members that have indicated that they would scale back on offerings directed to children should such change be adopted.

Promotions operators also rely on the one-time use exception to provide a basis for collecting a friend's e-mail address to enable a child to send an e-card, invite or other online communication to a friend. The friend's e-mail address is clearly OCI. FAQ #44 provides: "In order to take advantage of COPPA's one-time contact exception for your e-cards, your webform may only ask for recipient's email address (and, if desired, sender and reciepient's first name and last initial)." Proposed new Section 312.5(c)(3) limitation of the exception to collecting "a child's OCI" does not seem to cover the collection of a friend's e-mail address, because we presume "a child" means the disclosing party not a third party, and even if it means other children there would be no way to know if the recipient e-mail belongs to a child or an adult. Again, eliminating the one-time use exception for e-card tools would likely result in the elimination of much of these free, fun and harmless activities for children.

We trust these apparent results of the language change were not the intent of the Commission and this problem can be fixed by reverting to the original language of "OCI from a child" not "a child's OCI." If the change was intentional, PMA respectfully submits that it is beyond the Commission's authority and directly contrary to Section 1303(b)(2)(A) of the Act, which states: "**online contact information** [OCI] **collected from a child** that is used only to respond directly on a one-time basis to a specific request from the child and is not used to recontact the child and is not maintained in retrievable form by the operator."[7] The change of "OCI from a child" to "a child's OCI," we respectfully submit, violates the Act's clear mandate.

3. Proposed Additional Exception to Verifiable Parental Consent (Section 312.5(c). The proposed change to Section 312.5 would allow operators to collect a parent's OCI to inform them about activities by their children that do not require verified parental consent. The PMA is in support and urges expansion.

The Commission proposes to amend Section 312.5(c) to add an additional exception to obtaining verified parental consent for collecting a parent's email address where such information will only be used to inform and update parents about their child's online activity. This exception would apply where the child's participation in a website or online service does not otherwise collect, use, or disclose children's Personal Information. As the Commission notes, allowing the collection of contact information for a very limited notification purpose on a site that does not otherwise collect Personal Information is "reasonable and should be encouraged."[8]

The PMA agrees with this proposal and suggests that the Commission apply it in other areas as well. As explained elsewhere in these comments, PMA strongly opposes the discontinuation of valuable tools for parental notification, such as E-Mail Plus. PMA would urge the Commission, should it decide to discontinue use of such practices as proposed, to consider expanding the applicability of the new exception to apply to situations in which the collection of the information is for a specific single use, such as prize fulfillment in a sweepstakes.

We note further that the practical usefulness of this additional exception is limited by the Commission's proposed expansive definition of Personal Information (e.g., screen names and photos). Indeed, it is activities like controlled chat that does not permit disclosure of Personal Information and moderated user-generated content contests (where the screening eliminates photos, videos or audio files that include Personal Information) for which this new exception has been requested. The net effect of the Commission's proposals is to make this new exception less meaningful than what was sought. For this reasons too, we urge the FTC to reconsider those changes.

[7] 15 U.S.C. Section 6502(b)(2)(A).
[8] NPR at p. 73.

4. Proposed Changes to Online Notice § 312.4(b). The FTC proposes a new requirement that online notices by operators include identification of all operators collecting Personal Information on a site or service, not just the main operator of the site. The PMA objects for several reasons. First, as discussed in more detail below, there is little evidence on the record to justify this proposal. Second, the proposed requirement is vague and unclear. Last, the requirement is likely to cause confusion and place an onerous burden on the primary site operator.

The Commission states in the NPR that it "believes that the identification of each operator will aid parents in finding the appropriate party to whom to direct any inquiry."[9] The PMA is not aware of, and the Commission has not cited in the NPR, any evidence demonstrating problems or difficulties with parents contacting the appropriate operator of a website or online service or that operators have abused the protocol that is currently in place. Further, to the PMA's knowledge, not one of the Commission's COPPA enforcement cases has addressed this issue. If the Commission has such evidence or actual concerns, the PMA encourages that it be presented as part of the public record in this matter, so that interested parties may review and comment on that evidence. Otherwise, the PMA does not see the need to amend the COPPA Rule on this issue.

Further, this requirement fails to recognize the realities of modern site ecosystems and would place an unfair burden on a site operator that operates the site or application in compliance with the COPPA Rule, but that also hosts other third party applications and services. As advertising networks and other entities that may have a presence on a website may change frequently, maintaining and updating the specific contact information for such parties would be quite onerous, if not impossible, for a website operator to manage. Rather than implementing a drastic change to the COPPA Rule that is not supported with credible evidence as being a problem, PMA encourages the Commission to continue to allow operators to act as liaisons between third parties who may have a presence on the site and the consumers who visit their site. Dedicating one operator as a contact for parents gives them a single responsible party and removes any question as to where they should direct their inquiries. In this regard, PMA suggests that the FTC clarify its intention as to what parties it believes are "operators" and thus should be identified to users, so that any proposed change in this area does not place additional, and unwarranted burdens on the actual operators of a website or online service.

[9] NPR at p. 49.

In addition, the Commission's proposed language is extremely vague as to what operators would be covered by this requirement and what information would be required. For example, the proposed language would effectively cover all operators on a website, not just those that collect children's information ("each operator of a website or online service."[10]). As a result, rather than streamlining the disclosure process, this could provide parents and guardians with too much information, and make it more difficult to pinpoint the appropriate contact, should that be necessary. Further, an entity that operates a website or has a presence on a website hosted by another that does not collect children's information covered under the COPPA Rule should not be required to be identified nor provide their contact information on the website. If the Commission finds there is sufficient and credible evidence on the record that warrants this change, the PMA respectfully suggests that only entities that collect information covered by a COPPA obligation to obtain verified parental consent be required to comply.

As an alternative approach, the PMA suggests that the Commission consider clarifying that an entity with a presence on a website or online service that itself collects or attempts to collect Personal Information from children, but is not the primary operator, should be identified and obligated to comply with the COPPA Rule, at the time such information is collected or requested. In addition to addressing and furthering the Commission's interest in identifying relevant entities that collect information on a covered website, this "just in time" approach is consistent with the Commission's position on privacy matters generally, as detailed in its Staff Report.[11]

The suggested approach would address and further the Commission's interest in providing consumers with just the information they need and not more, so as to maintain and not dilute the importance of the provided information. Indeed, the Commission has noted in the NPR and elsewhere, that there are times when providing consumers with less, but more material, information may prove more valuable as such information will likely be seen, read and understood by consumers, rather than providing too much information. PMA notes that this approach echoes the point advanced by the FTC in its December 2010 Staff Report regarding consumer privacy, in which it states: "Privacy policies have become longer, more complex, and, in too many instances, incomprehensible to consumers. Too often, privacy policies appear designed more to limit companies' liability than to inform consumers about how their information will be used." [12] The PMA is concerned that the new requirement as proposed by the FTC will obfuscate the important information this requirement is intended to convey.

[10] NPR at p.51
[11] Id. at p. 64.
[12] Preliminary FTC Staff Report, Protecting Consumer Privacy in an ERA of Rapid Change ("Staff Report"), at p. 19.

5. New Categories of Personally Identifiable Information

The FTC proposes that ZIP + 4; pictures, audio tapes and videos submitted by children; unique identifiers (e.g., IP address, UDID, etc.) for uses other than "to support the internal operations of the website or online service [which is expanded to include "activities necessary to protect the security or integrity of the website or online services"]; geo-location data; and screen name (without combination with other Personal Information) should be treated as Personal Information, and questions whether date of birth, gender and ZIP codes should be treated as Personal Information. The PMA objects to any changes to the current definition of Personal Information.

The FTC proposes expanding the definition of Personal Information in several ways, including:

- Expanded Definition of "Online Contact Information" ("OCI")

Currently, the COPPA Rule specifically addresses e-mail addresses, screen names that include e-mail addresses, and instant messaging (IM) handles. The proposed new definition of "online contact information" would include any identifier that permits direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier. Part of this shift would be to include a new definition for "screen name" and treat it now as *per se* Personal Information. As explained below, the PMA submits that the Commission's proposal goes too far and, as a result, children will lose the ability to engage in valuable activities absent verified parental consent. The increased time and costs associated with doing so will likely result in our members discontinuing certain activities available to children.

- New Definition for Screen Name

Currently, the COPPA Rule considers a screen name to be Personal Information only if it includes an e-mail address. This should remain the rule. The Commission's proposal would capture all screen names that are used for any purpose "other than support for the internal operation of the website or service", a term it defines to include only activities that are "*necessary* to maintain the technical functioning of the site, to protect the security or integrity of the website or online services, or to fulfill a request of a child as permitted by [other sections]."[13] Thus, a third party social network user or screen name (e.g., a Twitter handle) would be considered Personal Information under the rule if a website uses those for login purposes (instead of setting up its own registration system). Even more problematic, this could be read as prohibiting use of screen name with respect to onsite activities that enable users to interact even if they cannot disclose Personal Information (e.g., controlled chat). Treating screen names in this manner (if intended) appears to be overreaching, and the Commission has not suggested any harm that needs to be addressed by the proposed *per se* treatment of screen and user names as Personal Information.

[13] NPR at p. 37 (emphasis added).

The exemption for internal use would appear to apply only in cases where a screen name is necessary to maintain the technical functionality of a website. It is not clear what this exemption really permits and we urge clarification. Of course, use of the account name or handle combined with Personal Information (*e.g.*, first and last name, e-mail address, etc.) is Personal Information. As currently proposed, it is not clear that "support for the internal operations of the site" would allow use of screen names for users to be indentified by other users for on-site controlled chat. Tens of millions of kids chat and interact with each other on sites that do not permit kids to post Personal Information where there was no verified parental consent. The FTC has proposed to expand this type of chat by eliminating the 100% deletion standard and allowing use of filters, etc. that eliminate the ability to post most Personal Information. However, if an operator needs verified parental consent to identify users using such a chat function (which would be by user name or screen name), the expansion is meaningless. Further, looking at the expanded definition of OCI (absent clarification otherwise), screen name for onsite chat, even safe chat, is OCI and thus Personal Information. The Commission's commentary states that a screen name can be used to "identify users to each other" is still acceptable as non-personal information,[14] but if you can identify and contact, even if that contact is via a chat function that is limited by drop down choices or filters to prevent disclosure of Personal Information, it would seem to fall within the new definition of OCI because it "permits direct contact with a person online". If this is the case, children that are currently using controlled chat would not be able to use these services absent getting verified parental consent and the proposed expansion of filtered chat is really no expansion at all. We assume this is not the FTC's intent and urge a clarification. Even if it is the Commission's intent and such a change should go into effect, the change should be prospective only for new users to avoid disruption of controlled chat for millions that entered under the existing scheme.

- Persistent Identifiers

The FTC proposes to add a new definition as follows:

"A persistent identifier, including but not limited to, a customer number held in a cookie, an IP address, a processor or device serial number, or unique device identifier, where such persistent identifier is used for functions other than or in addition to support for the internal operations of a website;" and

"An identifier that links the activities of a child across different websites or online services."[15]

In advancing this new definition and treating it as *per se* Personal Information, the FTC posits that unique identifiers personally identify individuals as opposed to identifying devices that are used by individuals. Furthermore, the Commission fails to acknowledge that many operators operate families of sites and have a legitimate reason for tracking their users across their online services (e.g., interrelated apps and sites) and that requiring verified parental consent for this purpose will create burdens not offset by mitigation of any real harm.

[14] NPR at p. 30.
[15] NPR at p. 36-37.

The PMA respectfully suggests that the Commission is wrong in its conclusion that device identifiers do not merely identify devices but rather personally identify people. Treating persistent identifiers as Personal Information offers negligible increased protections to children and would likely be unworkable in a practical sense. Courts have consistently found that an IP address applies to a computer not a person. *Johnson v. Microsoft Corp*., No. C06-0900 RAJ, 2009 WL 17934400 (W.D. Wash. June 23, 2009) ("When a person uses a computer to access the Internet, the computer is assigned an IP address by the user's Internet service provider."). Computers may be shared by an entire family or, in the case of libraries and other public use computers, an entire community. Furthermore, an IP address or UDID alone does not transmit any sensitive information. If Personal Information is associated with a persistent identifier then it becomes Personal Information, but not before. In addition, unlike the submission of a child's name or address, an IP address is transmitted automatically upon any individual's accessing a web page. *Klimas v. Comcast Cable Commc'ns, Inc*., 465 F.3d 271, 276 n.2 (6th Cir. 2006) ("IP addresses do not in and of themselves reveal 'a subscriber's name, address, [or] social security number.'"). In addition, an IP address is collected automatically by all web servers when they serve a web page to a computer. There is no ability to serve the web page without "knowing" the IP address where to send it. Thus, even for a web site directed toward children, it is technologically impossible to obtain parental consent prior to collecting an IP address. This makes the treatment of IP addresses as Personal Information under COPPA unworkable as part of the type of verified parental consent scheme that is the heart of COPPA. We note that the Commission attempts to provide for some uses of persistent identifiers that do not require verified parental consent. However, as noted above, it does not explain what is and is not included in "activities *necessary* to maintain the technical functioning of the site or online service [and] to protect the security or integrity of the website or online service…."[16] Indeed, what will the standard for determining necessity be? At minimum, there needs to be more guidance on what so-called internal uses will be acceptable under this exception.

As an example, the Commission states that "The new language in the definition would permit operators' use of persistent identifiers for purposes such as user authentication, improving site navigation, maintaining user preferences, serving contextual advertisements, and protecting against fraud or theft. However, the new language would require parental notification and consent prior to the collection of persistent identifiers where they are used for purposes such as amassing data on a child's activities or behavioral targeting advertising to the child."[17] This suggests acceptable and unacceptable internal uses with no guidance on where the line is drawn. Given the complexity of online services (such as multi-level games), operators need to "amass data on a child's activities" to optimize the services. They similarly need to amass significant activity data to provide contextually relevant content and ads. The FTC does not clarify where the line is drawn between permitted data tracking and collection for internal purposes and amassing too much data, even if for internal purposes and clarification is needed. Also, the Commission attempts to draw a line between "contextual" and "behavioral" advertising, with identifiers used for "contextual" advertising being permissible while identifiers for "behavioral" advertising requiring prior verified parental consent. This seems like a distinction without a difference, as all "contextual" ads depend upon some action taken by the computer user (*e.g.*, entering a search string, viewing certain content, engaging in certain activities) - this sounds an

[16] Proposed definition of "Support for the internal operations of the website or online service" (emphasis added).
[17] NPR at p. 37.

awful lot like "behavioral" advertising and the FTC does not explain how it interprets the difference between the terms. A blurring of the lines in this regard would likely be problematic. Any advertising that uses persistent identifiers and/or cookies and other tracking technologies to tailor the relevancy of the message may arguably require prior parental notice and consent under the confusing guidance the Commission has offered.

- Audio and Video Files and Photos

The FTC intends to apply the COPPA Rule to any "photograph, video or audio file where such file contains a child's image or voice." The Commission has already made it clear that such content will be Personal Information if such files are combined with any other form of Personal Information or information that would permit contact. The NPR provides no examples of any harm that has come from allowing children to post their image or voice where such has been screened to ensure that no Personal Information is included. Rather, the FTC expresses concern about the "privacy and safety implications of such practices" and states that "photos can be very personal in nature."[18] Under COPPA, "Personal Information" is not information that is personal, but that "the Commission determines permits the physical or online contacting of a specific individual."[19] The Commission's concern that some photos may contain geo-location information, and by implication that might enable the ability to contact the individuals depicted, is as speculative as its statement that "facial recognition technology can be used to further identify people depicted in photos."[20] We submit that the FTC's proposal exceeds its statutory authority under both COPPA and Section 5 of the FTC Act. While it may be a best practice for operators to at least give parents notice and an opportunity to remove posted pictures and video or audio files that do not include Personal Information, there is no authority to support imposing an obligation for them to obtain verified parental consent. Also, this change would likely result in diminished or eliminated submissions of user-generated content, even that which is screened and moderated, for children in many instances and in particular free promotional campaigns like send-to-friend e-cards and photo contests.

- Geo-location Data

The proposed revised COPPA Rule would include geo-location data in the definition of Personal Information - just the same as a home address. Apparently the Commission believes that because a device "checked in" somewhere, this permits individual contact. This is just not the way typical geo-location works on mobile devices. One can "check in" at a place far from the person's home location at a given time. That's usually the point of those sorts of promotions. "Checking in" shows off where a person has been at a particular moment -- the more exotic, the better. How is it that one's "checking in" at Machu Pichu in Peru allows individual contact with the person, whose primary residence is actually in Washington DC? Even though the proposed addition is limited to geolocation data "sufficient to identify street name and name of city", due to the inherent nature of mobile media, a device's location would change constantly as the owner of the device moves around. Further, not only is geo-location fleeting, it is not precise. For

[18] NPR at p. 39.
[19] 15 U.S.C. Section 6501(8)(F).
[20] NPR at p. 40.

instance, checking in at the Super Bowl may indicate street and city, but it is not reasonably personally identifiable information that would allow direct contact.

- DOB, Gender, ZIP+4

The Commission asks if it should also include date of birth, gender, ZIP+4 or other information as Personal Information. This type of data is not personally identifying and serves legitimate purposes of marketers and operators, such as the ability to serve contextually relevant content and ads. The Commission has not suggested that any harm has resulted from its collection and use. If the FTC has such evidence, PMA submits that this information be shared with the public and seek further public comment regarding its relevancy.

CONCLUSION

The PMA supports reasonable efforts to protect children and maintain parent's reasonable expectations of privacy for their children using ever-evolving online media and technology. PMA appreciates the FTC's review of the COPPA Rule and its efforts to keep it relevant. Our members are, however, concerned that some of the proposed changes, such as elimination of E-Mail Plus, are merely to promote innovation rather than to address any harm, and will result in additional costs for industry that will reduce content available to children. Other changes may too have unintended effects, such as the proposed language change to the one-time use exception, and as such, PMA seeks clarification that the one-time use exception remains available for contacting parents to get an address to send a prize and for facilitating e-cards sent by children. PMA is also concerned about treatment of additional categories of information as *per se* Personal Information when they cannot in many instances enable personal identification or contact and we find the carve outs for internal uses to be too restrictive as written and in need of further expansion and clarification. If any of these material changes are implemented, we urge a prospective implementation (i.e., “grandfather” existing users), and sufficient time to develop new site tools and activities before the new rules go into effect. We trust that the Commission will take these comments and concerns into account in finalizing the COPPA Rule revisions.