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

In the Matter of Children's Online Privacy Protection Rule; Supplemental Notice of Proposed Rulemaking	)	COPPA Rule Review 16 CFR Part 312 Project No. P104503

To: The Commission

COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®

Michael F. Altschul
Senior Vice President, General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

Krista L. Witanowski
Assistant Vice President, Regulatory Affairs

CTIA-The Wireless Association®

Dated: September 24, 2012

TABLE OF CONTENTS

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

In the Matter of Children's Online Privacy Protection Rule; Supplemental Notice of Proposed Rulemaking	)	COPPA Rule Review 16 CFR Part 312 Project No. P104503

To: The Commission

COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®

CTIA – The Wireless Association® ("CTIA")[1] hereby submits these comments in response to the Federal Trade Commission's Supplemental Notice of Proposed Rulemaking[2] concerning the Children's Online Privacy Protection Act ("COPPA").[3] The Commission proposes to amend its rules implementing COPPA ("Rules" or "COPPA Rules") by modifying the definitions of "operator," "Web site or online service directed to children," "personal information," and "support for internal operations."

Certain proposed revisions to COPPA Rules go beyond the scope of the statute and will result in significant unintended consequences, including stifling innovation, decreasing overall

[1] CTIA is an international nonprofit industry association representing the wireless telecommunications industry since 1984. Members of CTIA include wireless carriers and suppliers, as well as providers and manufacturers of wireless data services and products. CTIA coordinates the industry's voluntary efforts to provide consumers with a variety of choices and information regarding their wireless products and services.

[2] Request for Comment on the Federal Trade Commission's Supplemental Notice of Proposed Rulemaking, 77 Fed. Reg. 46643 (Aug. 6, 2012) ("Supplemental Notice"). References to "FTC" or "Commission" are to the Federal Trade Commission.

[3] Children's Online Privacy Protection Act, 15 U.S.C. § 6501 (1998).

privacy protections, and hindering the ability of children to participate in positive and valuable Internet-based experiences.

I. INTRODUCTION AND EXECUTIVE SUMMARY

Many of the privacy concerns highlighted in the Supplemental Notice have been and will continue to be addressed through industry self-regulatory efforts, as well as appropriate regulatory oversight. The wireless industry, in particular, has demonstrated its leadership and commitment to providing parents with the tools they need to understand and manage their children's use of mobile devices to, among other things, access the Internet-based web sites and online services addressed by COPPA. For example, CTIA and the Entertainment Software Rating Board ("ESRB"), along with six founding mobile application storefront operators and the app developer community, have created a mobile application rating system that allows developers to use a standard set of ratings. Parents can utilize the ratings, along with participating storefront filters, to control the app downloads of their children.[4] In addition, CTIA and The Wireless Foundation together sponsor "Growing Wireless," a website and set of resources devoted to helping parents understand mobile issues and better manage their children's device usage.[5]

Industry initiatives that apply to general audience and child-directed Web sites and online services alike protect many of the privacy rights addressed by COPPA and offer further

[4] *See CTIA Business Resources, available at* http://www.ctia.org/business_resources/wic/index.cfm/AID/12076 for more details regarding the CTIA Mobile Application Ratings Program with ESRB.

[5] *See* http://www.growingwireless.com/ for more details regarding Growing Wireless.

restrictions regarding the use of inappropriate content and sharing of certain types of data.[6] For example, CTIA has developed "Best Practices and Guidelines for Location-Based Services (LBS)" that guide service providers regarding the use of location-based data, including requirements for appropriate notice and consent.[7]

Experience shows that operators of Web sites and services directed to children are in the best position to give notice and obtain consent, and to control which plug-ins, software downloads, advertising networks, or other services are integrated into their sites or services. However, the Commission's proposed definitions for "operator" and "Web site or online service directed to children" may create unintended consequences by drawing third-party service providers into the Rule's scope, rather than placing the burden on first-party providers.

In addition, the Commission's "knows or has reason to know" standard is problematic and unworkable because it will create significant uncertainty among the industry that could cause companies to take unnecessary and counterproductive steps out of fear of liability. The Commission must take care not to impose an expansive standard, that is both open to significant interpretation and based on yesterday's technology, and which would result in the very real potential to grind many innovations to a halt. The "knows or has reason to know" standard also

---

[6] *Best Practices and Guidelines for Location-Based Services*, CTIA, http://www.ctia.org/business_resources/wic/index.cfm/AID/11300 (last visited Sept. 12, 2012) ("LBS Best Practices Guidelines").

[7] *See also, e.g.*, *Self-Regulatory Principles for Online Behavioral Advertising* and *Self-Regulatory Principles for Multi-Site Data*, Digital Advertising Alliance ("DAA"), http://www.aboutads.info/principles (last visited Sept. 12, 2012) (providing a principles-based approach to industry self-regulation for online behavioral advertising and the collection and use of information regarding web viewing over time and across non-affiliated web sites); *Code of Conduct for Mobile Marketing*, Mobile Marketing Association, http://mmaglobal.com/codeofconduct.pdf (last visited Sept. 12, 2012) (establishing a set of privacy standards for those who utilize user information to market products and services to those users via mobile devices).

could require third parties to affirmatively monitor content to ensure their compliance, adding to the privacy concerns associated with the proliferation of databases containing information identifying users and their activities.

CTIA supports the Commission's drive to modernize the definition of "personal information" to include screen or user names that may be used to contact a specific individual. However, the proposed expansion of personal information to include persistent identifiers that alone cannot be used to contact a specific individual goes beyond the scope of COPPA. This proposed change could also adversely impact innovation and service enhancements that parents and children find useful and desirable.

Lastly, depending solely on an enumerated list of exceptions regarding "support for internal operations" is unlikely to keep pace with technology and user demands. Exceptions should also be determined on a functional basis that focuses on how such information is used.

II. FIRST-PARTY PROVIDERS ARE BEST-POSITIONED TO MANAGE THE USER EXPERIENCE AND SUPPORT THE RULE'S OBJECTIVES.

The operator of a child-directed Web site or online service is in the best position to give notice, obtain parental consent, and control which plug-ins, software downloads, advertising networks, or other services are integrated into their sites or services. However, the Commission's proposed definition of "operator" lacks clarity where multiple parties are involved in delivering Web site content and services, as is frequently the case in today's Internet ecosystem. In this environment, the first-party provider who targets a Web site or online service to children is best-suited to manage the user experience and support the objectives of the COPPA Rule.

Unless the Commission's regime focuses COPPA compliance obligations on that first party who "owns" the user experience, parents will be barraged with a mass of confusing notice

and consent requirements. While parents will generally recognize first-party providers, they may not be familiar with the third parties who provide individual plug-ins, downloads or other services that the first party depends on to create a positive user experience. If presented with separate notices by each provider in the chain, parents will likely be confused and therefore may be hesitant to give consent – even where they trust the first-party provider – unnecessarily limiting their children's Internet participation.

The FTC also proposes that a first party who targets or directs its Web site to children and then "chooses" to integrate third-party services into its site or service that actually collect personal information "on its behalf" appropriately falls within the scope of "operator."[8] CTIA agrees to the extent that the FTC means to subject such first parties to compliance specifically and only where they affirmatively act to integrate such third-party services and have an established contractual relationship (e.g., agent, supplier) with such providers.

A. "Operator" should be defined to encompass only the first-party provider who targets a Web site or online service to children.

The Commission should define "operator" to include only the first-party provider that targets a website or online services to children. As described in CTIA's prior comments, in today's Internet ecosystem multiple entities and service providers are often involved in delivering content to the user and those entities may collect or access data deemed "personal information" under the Rule.[9] However, it is the first party who "targets" or "directs" the Web site or online service to children and that is best-positioned to support COPPA Rule obligations,

[8] Supplemental Notice, 77 Fed. Reg. at 46644.

[9] CTIA Comments, *In the Matter of Request for Public Comment on the FTC's Implementation of the Children's Online Privacy Protection Act Rule*, COPPA Rule Review, 16 C.F.R. pt. 312, Project No. P104503, at 16 (Dec. 23, 2011). ("CTIA Prior Comments").

particularly notice and consent, and to control which plug-ins, software downloads, advertising networks, or other services are integrated into their site or service.

In the Supplemental Notice, the Commission appears to generally support focusing on the first-party provider, at least in some situations. The Commission notes that a first party who targets or directs its Web site to children and then "*chooses"* to engage another provider to collect personal information "on its behalf" appropriately falls within the scope of "operator."[10] CTIA agrees that such first parties are rightfully encompassed by the Rule when they depend on others to actually collect information on their behalf or as a part of providing services to them, specifically and only where the first party affirmatively acts to integrate those services and has an established contractual relationship (e.g., agent, supplier) with such third parties. Conversely, third-party service providers who provide capabilities or features utilized by first parties, including the collection of personal information, should not be considered "operators," as users do not recognize any relationship with them.

Through its industry best practices and guidelines regarding location-based services ("LBS"), CTIA has tackled a similarly complicated issue involving multiple-party content delivery chains by focusing on the user's perspective and placing the compliance burden on first-party providers who are best-positioned to protect and support the user's experience and preferences.[11] CTIA defines an "LBS Provider" as *the* entity the user recognizes as having a direct relationship with him or her in the context of a specific service and so obligates first-party providers to give notice and obtain consent. The CTIA LBS guidelines do not require third-party providers to provide separate notice or obtain separate consent. For example, the developer of a

[10] Supplemental Notice, 77 Fed. Reg. at 46644.

[11] *See generally*, LBS Best Practices and Guidelines.

driving directions app that a user may download to her smartphone would be an LBS Provider, but the wireless carrier that provides location information to the app developer or the manufacturer of the smartphone is not an LBS Provider in this situation.[12] This user-centric approach provides a clear contact point for consumers and avoids the confusion created by multiple notice and consent requests by each entity in the service provider chain.

Likewise, in the COPPA context, limiting "operator" to specifically encompass only the first party would establish a single contact point for parents and provide certainty for the many players in the Internet ecosystem. For example, a gaming app developer may target its Web site or online service to children. That app developer is the first party and would be held accountable for COPPA Rule compliance as an "operator." If that first-party app developer then chooses to utilize infrastructure services from a third party cloud services provider, the first-party app developer would still be the only "operator," even if the third party's capabilities that are now incorporated into the app developer's Web site or service collect "personal information." Further, if the first-party app developer integrates a third party's social media features into its Web site or online service, it would still be the only "operator," even if the third party may access and use the information collected by its services. In all cases, the first-party would be required to provide notice and consent that encompasses its activities and those of the third parties whose services it chooses to integrate into its Web site or service offering.

By clarifying that the definition of "operator" only encompasses the provider who targets or directs a Web site or online service to children, the Commission has the opportunity to leverage the user-centric approach already adopted by industry, while still establishing clear accountability and compliance with the COPPA Rule. Fostering a consistent approach to

[12] *Id.* at Section 2 – Applicability.

managing privacy issues across similar, multi-party content delivery chains is paramount to ensure widespread user understanding and facilitate a positive online experience.

In the end, it is reasonable and consistent with the COPPA statute's purpose that the first-party provider of a Web site or online service directed to children, and not multiple providers of various component services, be bound as an "operator" under the statute's requirements. This approach creates a consistent, understandable user experience, especially for parents who are not familiar with the complex, multi-party content delivery chain.

B. Third-party providers do not have any reasonable means to know that a Web site or service is directed to children.

Organizations that participate in the content delivery chain, such as third-party providers who offer general audience services or collect information merely incident to the use of a particular site, do not have any reasonable or practical means to know that a Web site or service is directed to children. Therefore, it is reasonable to limit the COPPA Rule's scope to those first-party providers who "target" or "direct" a Web site or service to children, while excluding such third parties from direct liability.

For example, a cloud services provider that supports data collection and storage or web server capabilities has no practical way of determining when its services are being used to support child-directed sites. As described in Section III below, even if it was practical, obligating such service providers to employ technologies to monitor their services would intrude on the privacy of adults and children alike.[13]

In addition, entities that offer general marketplaces for applications should also not be considered "operators" unless the marketplace itself (or some portion thereof) otherwise meets the definition of a "Web site or online service directed to children."

[13] *See infra* at III.A.

Likewise, carriers, device manufacturers, and platform providers (e.g., operating system, browser software, etc.) should be specifically exempted from the definition of "operator," even if they collect information incident to the use of such sites, where such information collection is not specific to children or to the fact that the first-party provider's Web site or service is targeted to children. Platform providers regularly collect data related to connectivity, for diagnostic purposes, to monitor compliance with terms of use, or for other purposes and also have no practical way of determining when such data is being collected in connection with a visit to a child-directed site. Again, creating an obligation to monitor or review such services and determine if they are likely being used in connection with a child-directed site would intrude on the privacy of all users.[14]

III. CTIA SUPPORTS THE COMMISSION'S PROPOSED APPROACH TO MIXED USE WEB SITES AND SERVICES, BUT THE "KNOWS OR HAS REASON TO KNOW" STANDARD IS TOO VAGUE TO BE WORKABLE.

CTIA supports the Commission's pragmatic approach to mixed use Web sites and services as generally providing a good balance between industry impact and protection for children and families. However, CTIA cautions that the "knows or has reason to know" standard is too vague to be workable. The uncertainty created by such a vague standard will cause companies beyond advertising networks and plug-ins to take unnecessary and counterproductive steps out of fear of liability. What the proposed "knows or has reason to know" standard fails to

[14] If, despite these concerns, the FTC chooses to encompass third-party providers within the scope of COPPA liability, then the Commission should allow them to disclaim or exclude the use of their services by child-directed sites. However, while this may provide some relief to third-party providers, it is not the ideal answer because it could negatively impact the availability and capabilities of child-directed Internet services. First-party providers often integrate third-party services in their end user offerings to keep costs reasonable. Therefore, the lack of such services could easily stifle innovation by first-party providers and thwart creative, low cost business models that would otherwise deliver desirable child-directed content.

consider is that the Internet industry is composed of many interdependent companies many of which have little or no direct relationship with the end user.

Lastly, CTIA generally supports the FTC in its inquiry about technologies or standards that may be used to identify child-directed sites. CTIA cautions the Commission, however, that these technologies or standards should not be mandated and technologies that "tag" or "signal" specific Web sites or traffic may diminish privacy for all users.

A. The "knows or has reason to know" standard is too vague to be workable.

The "knows or has reason to know" standard is too vague, and has the potential to unintentionally sweep in third parties that simply have access to information incident to the use of first-party Web sites and services. For example, a third party could conceivably have "reason to know" through some type of undefined analytical means that personal information might be collected through a Web site or online service directed to children. As a result, third parties, as a practical matter, may need to affirmatively monitor content to ensure their compliance, adding to the privacy concerns associated with the proliferation of databases containing information identifying users and their activities.

As expressed above, CTIA raises similar concern about the proposed definition of "operator," which may also create unintended consequences. The Commission must look at these two issues in tandem and adopt a consistent approach that places the Rule's burden on the first party.

The Commission states that a "reason to know" standard "does not impose a duty to ascertain unknown facts, but does require a person to draw a reasonable inference from information he does have."[15] Despite the Commission's attempt to provide assurance regarding

[15] Supplemental Notice, 77 Fed. Reg. at 46645, n.18.

the limited scope of this standard, CTIA remains concerned that its application will be problematic. For example, Comment (d) of Section 9 of the Restatement Second of Agency explains that:

> A person has reason to know of a fact if he has information from which a person of ordinary intelligence, or of the superior intelligence which such person may have, would infer that the fact in question exists or that there is such a substantial chance of its existence that, if exercising reasonable care with reference to the matter in question, his action would be predicated upon the assumption of its possible existence. The inference drawn need not be that the fact exists; it is sufficient that the likelihood of its existence is so great that a person of ordinary intelligence, or of the superior intelligence which the person in question has, would, if exercising ordinary prudence under the circumstance, govern his conduct as if the fact existed, until he could ascertain its existence or non-existence.[16]

Terms like "ordinary intelligence," "superior intelligence," "ordinary prudence" and "reasonable care" do not provide sufficient clarity for companies to follow.

Equally troubling, in summarizing what "reason to know means," the Commission states that "sites and services will not be free to ignore credible information brought to their attention indicating that [their services are incorporated into child-directed properties]."[17] However, the term "credible" is not defined. In addition, the Commission does not explain what it means to collect information "through a host Web site or online service."[18] For example, can a service

[16] Restatement (Second) of Agency, § 9, comment (d) (1958) (emphasis added); *see also* Restatement (Second) of Torts, § 12, comment (a) "'Reason to know' means that the actor has knowledge of facts from which a reasonable man of ordinary intelligence or one of the superior intelligence of the actor would either infer the existence of the fact in question or would regard its existence as so highly probable that his conduct would be predicated upon the assumption that the fact did exist."; Restatement (Second) of Torts, § 401, comment (a) "The words 'reason to know', are defined in § 12(1) and are used to denote the fact that the actor has information from which a person of reasonable intelligence or of the superior intelligence of the actor would infer that the fact in question exists or that such person would govern his conduct upon the assumption that such fact exists."

[17] Supplemental Notice, 77 Fed. Reg. at 46645.

[18] *Id*.

provider, software provider, or device manufacturer be subject to liability simply because a user types a Web address into her Internet browser and that provider or manufacturer collects some information related to the user's Web experience pursuant to established business practices?

In addition, the fast-paced Internet industry is constantly creating new technologies that do not fit the mold of regulatory frameworks based on yesterday's technologies. A case in point is the growth of cloud services providers. Cloud services providers, or their sub-contractors, agents or vendors may collect "personal information," under the Commission's proposed definition, incident to providing services to a first party, but in a manner that is invisible to the user (e.g., IP addresses, cookies or other data required to implement functionality the user wants such as secure data storage or ready access to stored data). In addition, such third-party cloud services providers may even run the risk of being considered "operators" themselves under the proposed changes to COPPA.

If a cloud services provider could, through some theoretical analytical process, potentially "know or have reason to know" that certain of its customers use its services to provide child-directed Web sites, it may decline such business for fear of being subjected to the COPPA rules. Cloud services providers also may feel obligated to deploy technologies that monitor users' activity and create their own system for authenticating a user's age online and/or obtaining parental consent. Even if the service provider were willing or able to afford deploying such technology, they would negatively impact the privacy rights of both adults and children by scanning data, monitoring usage or otherwise intruding into the user's experience. In fact, limiting the availability of cloud services to operators could easily result in fewer positive Internet experiences for children, especially since cloud services solutions are the cost-effective

choice of many, including small businesses and others with limited information technology skills or resources.

Similarly, carriers and manufacturers are particularly concerned that an expansive reading of the proposed "reason to know" standard, definition of "operator," and language in the Supplemental Notice could create liability for each entity in the Internet ecosystem. For example, applying a "reason to know" standard could result in manufacturers of smartphones second-guessing both their customers and first-party Web site operators out of concern that they could be considered to be collecting personal information through a Web site or online service directed to children. As with cloud computing, manufacturers could ultimately feel compelled to monitor users' activity and create their own system for authenticating a user's age online and/or obtaining parental consent. These measures would undoubtedly impose a monumental burden on adults' online experience and infringe upon their privacy rights. In addition, it is unclear how much additional protection such potential actions by manufacturers would provide to children given that generally only adults can purchase a smartphone in the United States.

B. Caution should be exercised in developing tagging technologies or standards that identify child-directed websites or services.

CTIA supports the FTC in its inquiry about technologies or standards that may be used to identify child-directed Web sites or online services.[19] However, CTIA cautions that such mechanisms must not be mandated or be used to limit the flexibility of service providers, device manufacturers and general audience Web sites and services. Technologies that are used to "tag" or "signal" that a specific Web site or traffic is directed to children may require additional levels of monitoring by service providers. This would undoubtedly diminish privacy for all users. In addition, any requirement enforced by the government involving the tagging or labeling of

[19] Supplemental Notice, 77 Fed. Reg. at 46652.

content can raise significant First Amendment concerns and/or result in a repressive regulatory regime that requires the government to make judgment calls about whether specific content qualifies for tagging. Instead, technologies or standards should focus on helping parents monitor and control their children's activities.

IV. THE PROPOSED DEFINITIONS OF "PERSONAL INFORMATION" AND "SUPPORT FOR INTERNAL OPERATIONS" ARE PROBLEMATIC.

CTIA supports the FTC's efforts to modernize the definition of "personal information" and include screen or user names that may be used to contact a specific individual as reasonable and consistent with the COPPA statute. But the proposed expansion of personal information to include persistent identifiers that cannot be used on a stand alone basis to contact a *specific* individual goes beyond the scope of COPPA.

Further, creating an enumerated list of exceptions regarding "support for internal operations," as the Commission proposes, is unlikely to keep pace with technology and user demands. The Commission should reconsider its approach and focus instead on protecting children's privacy interests regarding information that can be used to make *specific*, individual contacts, as defined under the statute. Alternatively, regulating the "uses" of personal information, rather than focusing on its collection, may assist the Commission in creating a better long-term strategy. Similarly, the Commission should be wary of expanding the definition of "personal information" to include persistent identifiers that are not used to contact an individual child.

A. By proposing to include persistent identifiers that cannot be used on a stand-alone basis to contact a specific individual child, the Commission exceeds COPPA's statutory boundaries.

As CTIA and others emphasized in their prior comments, Congress did not intend for stand alone "identifiers" (including "persistent identifiers") to qualify as "personal information,"

unless they permit a *specific* individual to be contacted physically or online.[20] The Commission exceeds COPPA's statutory boundaries by including persistent identifiers that cannot be used on a stand alone basis to contact a specific individual within the scope of "personal information."

Under Section 6501 of the COPPA statute, the definition of "personal information" includes five specific types of information and two broad categories.[21] Assuming that an "identifier" is not a first and last name; a home or other physical address including street name and name of a city or town; an e-mail address; a telephone number; or a Social Security number, and is not combined with one of these five specific identifiers, the FTC's statutory authority to categorize it as "personal information" is limited by Section 6501(8)(F). Under this subsection, the identifier must "permit[] the physical or online contacting of a *specific* individual."[22]

COPPA's legislative history makes clear the intent of the statute, which, as explained by COPPA co-sponsor Senator Richard Bryan (D-NV), is to control "attempts to communicate

---

[20] *See, e.g.,* CTIA Prior Comments at 6; *see also* the following comments submitted previously in *In the Matter of Request for Public Comment on the FTC's Implementation of the Children's Online Privacy Protection Act Rule*, COPPA Rule Review, 16 C.F.R. pt. 312, Project No. P104503: Microsoft Comments at 8-9; AT&T Comments at 6-9; Verizon and Verizon Wireless Comments at 3-5.

[21] 15 U.S.C. § 6501 (8). Personal information. The term "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 e-mail 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.

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

directly with a specific, identifiable individual."[23] Senator Bryan further added that: "[a]nonymous, aggregate information – information that cannot be linked by the operator to a specific individual – is not covered."[24]

Moreover, by including stand alone identifiers within the scope of "personal information," the FTC is acting inconsistently in its drive to update the definition. The Commission reasonably incorporated screen or user names where they rise to the level of "online contact information."[25] Such data elements meet COPPA's statutory requirements, because they may be used to contact a specific individual. However, in contrast, stand alone identifiers (e.g., IP addresses, cookies, device identifiers) do not rise to the same level, because on their own they cannot be used to contact a *specific* user.

Including a persistent identifier when it "can be used" to recognize a user over time or across different websites also is troublesome and unsupported by the statute. As technology evolves, this limitation will become increasingly meaningless, as more and more identifiers "can" potentially be used to "recognize" some user with the assistance of technology and various analytical means. This mere possibility should not be sufficient. More fundamentally, just because an identifier "can be used" does not mean that such an identifier is being used for the "physical or online contacting of a *specific* individual" as called for by the statute.

The Commission's categorical example of behaviorally-targeted advertising as contacting a specific individual is similarly misplaced, because such activities may be based on stand alone

[23] 144 Cong. Rec. S11657 (daily ed. Oct. 7, 1998) (statement of Sen. Bryan).

[24] *Id*.

[25] Supplemental Notice, 77 Fed. Reg. at 46646.

identifiers, user profiles or other characteristics and not individually identifiable data that would allow a *specific* individual to be contacted.

B. Any exception regarding "support for internal operations" should be defined on a functional basis that focuses on how such information is used.

The Commission's proposed definition of "support for internal operations" is applicable only if the agency includes persistent identifiers within the definition of "personal information." If the Commission does in fact expand the definition of personal information in this manner, it should also define "support for internal operations" on a functional basis that focuses on how such information is used rather than create an enumerated list of exceptions.

As technology evolves and operators seek to introduce innovative features and satisfy user demands, the data necessary to support such increasingly sophisticated operations will necessarily expand and change. Therefore, using an enumerated list of today's common activities to define such an exception is inherently limited. In contrast, a functional definition focuses on how such information is actually used and is not only better able to support future needs, but also better able to fulfill the objectives of COPPA.

Accordingly, should such an exception be necessitated by the inclusion of persistent identifiers in the definition of personal information, CTIA recommends the FTC consider defining "support for internal operations" as:[26]

> Those activities necessary to provide, maintain or improve the functioning and protect the security or integrity of an Operator's products, networks, systems or services, including such third-party products, networks, systems, services or devices as may be used to deliver an Operator's Web site or online services, or to fulfill a request of a child as

[26] In its prior comments, CTIA proposed a similar functional definition. *See* CTIA Prior Comments at 15. CTIA now offers an updated proposal to address the Supplemental Notice's clarifications, especially regarding the definitions of "operator" and "Web site or online service directed to children," and to recognize the needs of all those who participate in the multiple-party content delivery chain.

> permitted by § 312.5(c)(3) and (4), where the information collected for such purposes is not used or disclosed for any other purpose.

In particular, as with this proposal, any functional definition should recognize the need for third-party providers to collect and use such data in support of the content delivery chain. While no one can fully anticipate the kinds of features and services that operators may be able to offer in the future, given the rapidly evolving nature of the Internet, a functional definition like this one focuses on how such data is used, and helps to minimize the limitations inherent in any enumerated list of activities.

C. Alternatively, operators should also be given an option to certify to the limited uses of collected information through a COPPA Safe Harbor.

Alternatively, operators also should be given an option to voluntarily and publicly certify to the limited uses of information they collect in support of internal operations through a COPPA Safe Harbor, including that the collected information will not be used for the purposes of physical or online contacting of a *specific* child.

Today, the COPPA regime includes a Safe Harbor program for industry self-regulatory guidelines, utilizing agency-approved third parties for verification. The Commission should either confirm that the existing Safe Harbor regulations are broad enough as currently written to allow an application for approval of a usage-based regime or amend the existing Safe Harbor regulations to specifically allow this type of approach. Permitting this type of flexibility is consistent with past efforts to protect children's privacy. Further, operators of Web sites and online services directed at children may already be familiar with current Safe Harbor programs, so an incremental extension, as suggested here, could potentially lessen the burden and further promote transparency and compliance.

V. CONCLUSION

Evolving technologies have enabled children and families to engage in many positive and valuable Internet-based experiences, but that same rapidly changing Internet ecosystem also carries the potential to impact the privacy of both children and adults. CTIA applauds the FTC's efforts in reviewing and proposing updates to the COPPA Rules and appreciates the Commission's further efforts to clarify its proposed definitions in its Supplemental Notice. However, certain proposed revisions to COPPA Rules go beyond the scope of the statute and will result in significant unintended consequences, including stifling innovation, decreasing overall privacy protections, and hindering the ability of children to participate in positive and valuable Internet-based experiences. Therefore, CTIA respectfully requests that the Commission take actions consistent with the positions discussed herein.

Respectfully submitted,

CTIA – The Wireless Association®

By: */s/Michael Altschul*

Michael F. Altschul
Senior Vice President, General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

Krista L. Witanowski
Assistant Vice President, Regulatory Affairs

CTIA-The Wireless Association®

Dated: September 24, 2012