**Before the**
**FEDERAL TRADE COMMISSION**
**Washington, DC**

| | | |
|---|---|---|
| In the Matter of Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Act Rule | ) ) ) ) ) ) | COPPA Rule Review 16 CFR Part 312 Project No. P104503 |

# COMMENTS OF CTIA - THE WIRELESS ASSOCIATION®

## TABLE OF CONTENTS

## I. INTRODUCTION AND EXECUTIVE SUMMARY

CTIA - The Wireless Association® ("CTIA")[1] hereby submits these comments in response to the Federal Trade Commission's ("FTC" or "Commission") request for public comments on its proposed revisions[2] to the Children's Online Privacy Protection Act Rule ("COPPA Rule" or the "Rule").[3] The COPPA Rule, which implements the Children's Online Privacy Protection Act of 1998, was enacted to help create a safer and more secure Internet experience for children as technology evolves and online activities become ubiquitous.[4] The Rule applies to operators of websites, online services, and mobile applications that are directed to children under 13, and to operators who have actual knowledge they are collecting personal information online from children under 13 (collectively, "Operators").[5]

Despite the fact that the Rule does not apply to certain types of short message service ("SMS") and multimedia ("MMS") text messaging, COPPA has implications for many types of wireless services and the products and services offered on wireless platforms. The FTC's proposed amendments to the COPPA Rule ("Proposed Rule") must strike an appropriate balance between the goal of further protecting children's online privacy while ensuring that Operators and associated service providers are not unnecessarily burdened with new obligations that substantially undermine technological innovation and restrict choices and raise costs for consumers, while doing little to further the laudable goal of protecting children's online privacy.

Several of the FTC's proposed changes raise significant concerns with respect to COPPA compliance and the FTC's general privacy framework. Specifically, the proposed expansion of

---

[1] CTIA - The Wireless Association® is the international association that has represented the wireless telecommunications industry since 1984. Members of the organization include wireless carriers and suppliers, as well as providers and manufacturers of wireless data services and products.
[2] Request for Public Comment on the Federal Trade Commission's Proposed Rule, 76 Fed. Reg. 59804 (Sept. 27, 2011) ("Proposed Rule").
[3] Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 (1998).
[4] COPPA Rules, 76 Fed. Reg. 59804.
[5] *Id.*

the definition of personal information requires clarification. CTIA is particularly concerned that the Commission may have exceeded its statutory authority with respect to expanding the definition of personal information to include stand-alone identifiers. CTIA is also concerned that as currently drafted, the definition of personal information creates unintended consequences, particularly with respect to geolocation information; the proposed stand-alone list of identifiers; the expanded list of multimedia (*e.g.,* video, audio and photographs); the internal operations exemption; and the role of multiple Operators. Other provisions of the Proposed Rule, such as the new definition of "collect or collection," require clarification or should be reevaluated to ensure that the final rule is narrowly tailored so as to not stifle nascent technological and product innovations, including the adoption of HTML5 and cloud services. In addition, the proposed elimination of "email plus" as a consent mechanism should be reevaluated, particularly since the proposed consent mechanisms appear onerous and unworkable for both parents and Operators. The FTC's proposed changes to parental notice requirements with respect to multiple Operators should be less burdensome and more straightforward. Alternative methods of obtaining verifiable parental consent should be identified and endorsed. CTIA continues to support the text messaging exemption and the development of Safe Harbor programs that are straightforward to create and implement.

## II. THE EXPANSION OF THE DEFINITION OF PERSONAL INFORMATION IS PROBLEMATIC AND CREATES UNINTENDED CONSEQUENCES

The Proposed Rule unduly expands the definition of "personal information" so that more information such as persistent identifiers,[6] geolocation data, video, photographs, and audio files, *as stand-alone data elements,* will be covered under the definition. If adopted, this new definition will create uncertainty for many Operators and associated service providers not

[6] To further complicate matters, the FTC's proposed internal operations exemption: a) does not clearly include other related, legitimate uses of identifiers, b) creates additional compliance issues in the case of multiple Operators, and c) does not apply to other types of "non-persistent" identifiers. *See infra* Section III, pp 3-7.

currently subject to COPPA, particularly since the definition of "website or online service directed to children" may be expanded as well.

### A. Identifiers

Under the COPPA statute, identifiers qualify as "personal information" only if i) they permit contacting a specific individual or ii) they are combined with other personal information concerning parents or a child.[7] In the NPRM, the Commission contemplates whether the new COPPA Rule should cover persistent identifiers and identifiers that link the activities of a child across different websites or online services, even when such identifiers are not tied to other personal information.[8] The Commission discusses whether such identifiers would have to be used to contact a "*specific* individual" to qualify, and rejects the notion that persistent identifiers allowing Operators to potentially contact more than a specific individual are out of scope.[9] It states that the COPPA statute's reference to "permits the physical or online contacting of a specific individual"[10] does not mean "information that permits the contacting of only a single individual, to the exclusion of all other individuals."[11] Thus, it contends that device serial numbers and unique device identifiers ("UDIs"), as well as other persistent identifiers such as cookie IDs and IP addresses alone, should be considered personal information, even though these devices may be used by multiple people in a household, public library, school or Internet cafe.[12]

---

[7] 15 U.S.C. § 6501(8).
[8] Proposed Rule, 76 Fed. Reg. at 59810.
[9] Proposed Rule, 76 Fed. Reg. at 59811.
[10] 15 U.S.C. § 6501(8)(f); 76 Fed. Reg. at 59811.
[11] Proposed Rule, 76 Fed. Reg. at 59811.
[12] Proposed Rule, 76 Fed. Reg. at 59811-59812.

### 1. *Congress Did Not Intend the Definition of Personal Information to Include Stand-Alone Identifiers*

Congress did not intend for "identifiers" (including persistent identifiers) *as stand-alone data elements* to qualify as personal information, unless they permit an individual to be contacted physically or online. The COPPA statute defines **"personal information"** as:

> individually identifiable information about an individual collected online, including...(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.[13]

The fundamental criteria Congress clearly established in paragraph (F) with respect to personal information and other identifiers is that the "identifier" must permit a *"specific individual"* to be *"contact[ed] physically or online."*[14] Despite the clear intent of Congress, the Commission is attempting to expand the definition of personal information to include stand-alone identifiers that are not linked to other information and thus cannot be used *to contact an individual physically or online.* While Section 6502(8)(F) of the COPPA statute grants the Commission authority to modify the definition of personal information to include information such as identifiers that are not specifically listed in the statute, it does not grant the Commission unfettered authority. The Commission's goals in this proceeding are worthy, but any modifications to the definition of personal information must fall within the statutory framework and criteria Congress clearly articulated. Accordingly, CTIA is very concerned that the FTC lacks authority to expand the definition of personal information with respect to identifiers as stand-alone elements when such identifiers cannot be used to contact an individual physically or online.

[13] 15 U.S.C. §§ 6501 (8) (2010).
[14] 15 U.S.C. § 6502(8) (emphasis added).

### 2. *The FTC's Proposed Rule of Treating Persistent Identifiers as Personal Information Creates Unintended Consequences*

As the Commission correctly concluded in 1999, a persistent identifier does not equate to data that positively identifies an individual.[15] This fact still remains true. Unlike a telephone number, home address or email address, a persistent identifier such as a cookie ID, device ID, or an IP address does not identify an individual. That is why the Commission relies on the "permits online or physical contact" prong of the definition. A persistent identifier does not enable contacting an individual. For example, an entity that places a cookie on a device and later reads the persistent cookie ID cannot use that persistent ID alone to "contact" the individual. The entity would need more personal information to identify and contact the individual. At most, persistent identifiers facilitate later recognition of a device. Without the ability to contact or determine who the specific user is, it is unclear why stand-alone persistent identifiers should be deemed personal information. In view of such practical considerations, the Commission's tentative conclusions and its supporting rationale regarding personal information and persistent identifiers as stand-alone data elements is disconcerting and impractical.

Treating a persistent identifier alone as "personal information" also creates the unintended consequence that an Operator or its associated service provider would be deemed to have actual knowledge that an online visitor or user is a child, based simply on the persistent identifier itself. This is an illogical result. Moreover, websites and online services use IP addresses, cookies and other automated tools by necessity to deliver content to computers. If these tools, without more, are treated as personal information, an Operator would be liable for

---

[15] COPPA Rule's Statement of Basis and Purpose, 64 Fed. Reg. 59888 at 59892 (November 3, 1999), available at www.ftc.gov/os/1999/10/64fr59888.pdf (last visited December 19, 2011) ("One commenter noted that there are some persistent identifiers that are automatically collected by websites and can be considered individually identifying information, such as a static IP address or processor serial number. If this type of information were considered "personal information," the commenter noted, then nearly every child-oriented website would automatically be required to comply with the Rule, even if no other personal information were being collected. ***The Commission believes that unless such identifiers are associated with other individually identifiable personal information, they would not fall within the Rule's definition of "personal information.")***

collecting personal information as soon as a child visits a site's home page or screen if the tools do not qualify for the "internal operations" exemption.[16] These types of automated tools may be used for more than one purpose, and thus their inclusion as stand-alone data elements is unworkable and overbroad.

There are many legitimate uses of persistent identifiers and automated text. Reverse look-ups of IP addresses can identify a *general* geographic area and thus provide relevant information such as local news (for the nearest city), weather, and other topics of local interest. A unique identifier can also be used to gather service quality data ("SQM") or other analytics. SQM data does not have to be tied to an individual — to be useful, it only is necessary to know that it is coming from the same device. For instance, data gathered using an anonymous, randomly generated GUID ("Globally Unique Identifier") that persists on a device is helpful to determine that an activity (*e.g.*, a crash, a dropped call, an error) occurs ten (10) times on the same device, as opposed to one (1) time on each of ten different devices. It is not entirely clear whether this use of a persistent device identifier would fall under the "internal operations" exception.

Based on these concerns, CTIA respectfully requests that the Commission reconsider its proposed definition of personal information to ensure that the expansion of the definition is well within its statutory authority and does not create unintended consequences.

### B. Geolocation Information

CTIA agrees with the Commission that technological advances surrounding the collection, use, and disclosure of geolocation information raise important privacy and safety issues, and supports including it in the definition of "personal information" in the proposed

[16] Proposed Rule, 76 Fed. Reg. at 59830, § 312.2 (*amending Personal information* (g)).

amended Rule.[17] Important clarifications, however, are needed before adoption of the amended definition of "personal information" to include geolocation information.

### 1. *To Qualify as "Personal Information," Geolocation Information Must Be Tied To Other Personally Identifiable Information*

The Proposed Rule makes geolocation information "personal information" when it is merely identified to a street and city, but not to an individual home address.[18] Congress clearly limited the definition of "personal information" for COPPA purposes, to information that is "individually identifiable" and could allow an individual to be contacted.[19] Information pertaining to a street and city does not identify a household, much less a person.[20] Nor does stand-alone geolocation information that is not tied to any personally identifiable information facilitate such contact. By not defining persistent identifiers to mean information that ties geolocation data to an individual, nor relating it back to the underlying statutory purpose, the Proposed Rule impermissibly expands the requirement that covered information must be "individually identifiable."[21]

### 2. *The Commission Should Clearly Exclude Stand-Alone Geolocation Metadata*

CTIA agrees that opt-in consent should be obtained from a parent when his or her child's location is collected from a device. Requiring verifiable parental consent *whenever* geolocation data may be present, however, creates certain unintended consequences. As the Commission knows, stand-alone location information is sometimes embedded in metadata. For example,

---

[17] Proposed Rule, 76 Fed. Reg. at 59830, 16 C.F.R. § 312.2 (j) (*amending "personal information"*).
[18] *Id.* ("Personal information means … [g]eolocation information sufficient to identify street name and name of a city or town.")
[19] *Id.* at § 312.2 (*defining "personal information"*); 15 U.S.C. § 6501(8).
[20] This can become even more confusing in the context of an account with multiple users. *See CTIA Best Practices and Guidelines for Location-Based Services*, V2 at 4 (Mar. 23, 2010) (" CTIA Guidelines"), *available at* http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf.
[21] *Id.* at (g)(j); *see also* 15 U.S.C. § 6501(8).

most digital photographs contain geolocation data in metadata. [22] With photos stored in JPEG file format, for example, the geotag information is typically embedded in the metadata stored in Exchangeable Image File Format ("EXIF") or Extensible Metadata Platform ("XMP") format. This metadata is not visible in the picture itself but can be read and written by special programs and some digital cameras and modern scanners.

Requiring opt-in consent whenever geolocation data *may* be present creates the unintended consequence that COPPA would cover any online service that lets family members and other individuals post photos, such as Kodak[23] or Snapfish,[24] if such services do not exclude pictures or advertisements that depict children or otherwise may be of interest to children. This was not Congress' intent.

### 3. *Anonymous, Non-Personal Geolocation Data Should Also Be Excluded*

Anonymized data is data that can no longer be associated with an individual and yet may have ongoing use for Operators, *e.g.,* product and service development and service quality improvement. Once this data is stripped of personally identifying elements, those elements cannot be re-associated with the data or the underlying individual. In this context, the final Rule should clarify that the new 16 C.F.R. § 312.2(j) does not apply to *anonymous* geolocation data. Thus, the new COPPA regulations should: a) ensure that geolocation data covered by the proposed provision is tied to an individual, b) exclude geolocation metadata that may be present in photos and videos uploaded to "general audience" websites or online services, and c) clarify that anonymous geolocation data is not considered personal information.

---

[22] Considering 92% of smartphone owners use their phones to take pictures and 80% use their phones to send a photo or video to someone, this amendment could have major ramifications. Darrell M. West, The Brookings Institution, *Ten Facts about Mobile Broadband*(2011), *available at* http://www.brookings.edu/papers/2011/1208_mobile_broadband_west.aspx

[23] Kodak Picture Kiosk, http://www.kodak.com/global/en/consumer/kiosk/kioskMain.jhtml?pq-path=2301153 (last visited Dec. 15, 2011).

[24] Snapfish, at http://www.snapfish.com/snapfish/welcome.

### C. Photograph, video or audio file containing a child's image or voice

#### 1. *Proposed Definition Reaches Too Many General Audience Services and Websites*

The NPRM proposes broadening the definition of personal information to include "a photograph, video or audio file where such file contains a child's image or voice." CTIA is concerned that the Proposed Rule could be interpreted to extend to video or voicemail messages sent by children utilizing Skype,[25] Google Voice,[26] or similar websites or online services.[27] It is not clear at what point an Operator would have "actual knowledge that it is collecting personal information online from a child."[28] CTIA proposes a clarification that providers of general audience communications services and media sharing and uploading services, such as Picasa,[29] would not be imputed to have actual knowledge simply because the subject of the uploaded media includes a child's image or voice.

#### 2. *Other Unintended Consequences*

Without clarification, the Proposed Rule could also be interpreted to prohibit posting on Facebook a photo of a crowd that includes children at a professional baseball game or other public event unless consent is obtained for every child captured in that photo. For instance, would a parent be able to post a photo of her child's birthday party to a website like Snapfish without triggering a requirement that the Operator of the site obtain the consent from the parents of every other child in the photo? If the banner in the background of the photo says "Happy 7th Birthday," would that mean under the Proposed Rule that the Operator has actual knowledge that the children in the photo are under 13? The Proposed Rule may also encourage Operators of

---

[25] Skype, http://www.skype.com/intl/en-us/home (last visited Dec. 15, 2011).
[26] Google Voice, at https://www.google.com/voice/#history.
[27] Note that photographs, video, and audio files are not listed in the COPPA statute in the definition of personal information. 15 U.S.C. § 6501(8).
[28] 15 U.S.C. § 6502(a)(1).
[29] Picasa, http://picasa.google.com (last visited Dec. 15, 2011).

general audience websites and online services that allow posting and sharing of media to effectively censor content, out of fear that the display of pictures or audio content will trigger "actual knowledge." The Commission should also consider the impact on the Commission's stated goals of "preserving the interactivity of the medium, and minimizing the potential burdens of compliance on companies, parents, and children,"[30] and should follow the dictates of President Obama's regulatory review and cost-benefit analysis orders.[31] The FTC should articulate clearly the harms it is seeking to prevent or abate by the specific requirements of the Proposed Rule.

CTIA also seeks clarification from the FTC as to when actual knowledge is triggered in the cloud computing context. As discussed in greater detail in Section V.C., with cloud services it is difficult to discern which entity is actually "collecting" information and where it is going. Perhaps with the exception of certain types of Software as a Service ("SaaS") offerings, a cloud provider has no access to data collected via a website or online service. CTIA respectfully recommends that the Commission clarify in the final Rule that a cloud service provider is not deemed to have actual knowledge simply because it provides a platform, infrastructure or "back-end" software for a website or online service governed by COPPA.

Moreover, existing right of publicity laws[32] are effective in ensuring that parental consent is obtained for the use of images. These state laws already require parental consent for

[30] COPPA Rules, 64 Fed. Reg. at 59889, § 1.
[31] *See* Exec. Order No. 13,563, 76 Fed. Reg. 3821 (Jan. 21, 2011) ("Improving Regulation and Regulatory Review"), available at http://www.gpo.gov/fdsys/pkg/FR-2011-01-21/pdf/2011-1385.pdf. *See also* Exec. Order No. 13,579, 76 Fed. Reg. 41587 (July 11, 2011) ("Regulation and Independent Regulatory Agencies"), available at http://www.gpo.gov/fdsys/pkg/FR-2011-07-14/pdf/2011-17953.pdf.
[32] *See, e.g.* Cal. Civ. Code § 3344 and 765 I.L.C.S. § 1075.

commercial use of the photos and likenesses of minors[33] and protect children with respect to posting of images.

## III. INTERNAL OPERATIONS EXEMPTION

CTIA has raised specific concerns regarding the FTC's proposed expansion of the definition of personal information to include "persistent identifiers" as stand-alone data elements, particularly in view of the clear language of the COPPA statute, Congressional intent and the unintended consequences of the FTC's proposed approach.[34] Perhaps because the Commission recognizes the tension between its approach and the statutory language, the Commission is proposing to exempt persistent identifiers-used as "support for the internal operations of the website or online service" from qualifying as personal information.[35] Should the Commission determine, notwithstanding the clear language of the COPPA statute, that identifiers as stand-alone data elements are not personal information, then CTIA recommends that the Commission apply the exemption not only to persistent identifiers but also to other types of identifiers such as those contemplated under the proposed paragraph (h), including identifiers that "link[] the activities of a child across different websites or online services."[36] It is not clear from the NPRM why the Commission limited the proposed internal operations exemption to persistent identifiers and did not consider other identifiers.

CTIA recommends that the Commission also consider the numerous benefits that persistent identifiers and other types of identifiers provide Operators, parents and children. Certain identifiers, like IP addresses, are fundamental to the operation of the Internet. By way of

---

[33] For example, California's law states: "any person who knowingly uses another's name, voice, signature, photograph, or likeness, in any manner, on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods or services, without such person's prior consent, or, in the case of a minor, the prior consent of his parent or legal guardian, shall be liable for any damages sustained by the person or persons injured as a result thereof." Cal. Civ. Code § 3344(a).

[34] Section II.A, *supra,* at 3-7.

[35] *Id.* at § 312.2 (g) (*amending "personal information"*).

[36] Proposed Rule, 76 Fed. Reg. at 59812.

example, persistent identifiers – such as cookies, unique device identifiers or identifiers that link the online activities of a child across websites – allow Operators-and associated service providers to analyze website traffic patterns and determine which content is appropriate to deliver to children and parents. Such analytics can help Operators create walled-garden environments for children featuring age-appropriate content that is valuable to parents and educators. Persistent identifiers may also make it easier to comply with COPPA because they can help Operators identify devices that may be used by children. The Commission's FAQs encourage the use of temporary or permanent cookies for this very reason:

> ...we recommend that sites that choose to age-screen employ temporary or permanent cookies to prevent children from back-buttoning to change their age in order to circumvent the parental consent requirement or obtain access to the site.[37]

In addition, CTIA recommends that the Commission amend the definition of "support for the internal operations" to take into account the convergence of technology that has occurred since 1999. In particular, since 1999, with the growth of smart phones, online activities are now deeply intertwined with telecommunication technologies. So, although an Operator under the definition of the Act may be someone who operates a website or online service and collects information from users online, a mobile Operator's internal operations may include more than just online operations. For example, if a phone crashes, a mobile device manufacturer as part of its services may send the device identifier of the phone over the Internet to troubleshoot problems with that phone. Or, a wireless service provider may collect geolocation data from phones over the Internet to help determine where to install new cell towers.

CTIA also recommends that the Commission clarify that activities necessary to maintain the technical functioning of websites or online services include activities related to

[37] *Frequently Asked Questions about the Children's Online Privacy Protection Rule*, revised October 7, 2008, available at http://www.ftc.gov/privacy/coppafaqs.shtm (last visited December 20, 2011).

improvements to telecommunications hardware and systems. Accordingly, we would recommend that the term "support for the internal operations of the Web site or online service" be changed to "support for internal operations" and that this be defined as "those activities necessary to maintain or improve the technical functioning and protect the security or integrity of an Operator's products, networks, systems or services, or to fulfill a request of a child as permitted by § 312.5(c)(3) and (4), and the information collected for such purposes is not used or disclosed for any other purpose." This change will help support the Commission's goal of protecting users from security threats (not only online but throughout the entire ecosystem) and will allow Operators and associated service providers to develop improvements to telecommunications hardware and services that consumers demand.

Finally, the final Rule should recognize that identifiers are used for certain "commonly accepted" online practices. In the 2010 FTC Staff Report on Protecting Consumer Privacy ("Report"),[38] the Commission stated that it is "reasonable for companies to engage in certain practices – namely, product and service fulfillment, internal operations such as improving services offered, fraud prevention, legal compliance, and first-party marketing." For these "commonly accepted practices," the Report concludes that companies should not have to seek consent. These are precisely the types of practices that should be explicitly included in the internal operations exemption.

In sum, CTIA strongly encourages the Commission to adopt the proposed changes discussed above as equitable and justifiable exemptions to the Final Rule.

[38] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (December 1, 2010), available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (last visited December 20, 2011).

## IV. THE MULTIPLE OPERATOR ISSUE/ACCOUNTABILITY

An expanded definition of "personal information" also impacts who needs to provide notice to and obtain consent from parents. In many cases, multiple entities and service providers are interfacing with a single website or application, for example, by providing content or services, delivering advertisements, or rendering technical support or operational functionality. In order to provide one or more of these services, multiple companies may collect or access information using cookies or unique device identifiers that are not associated with other personally identifiable information.

The CTIA LBS Guidelines provide excellent examples demonstrating how multiple Operators and associated service providers may be involved in providing a service and how responsibility should be allocated. For example, a wireless carrier may be the *first-party* service provider when it directly provides users with an information service to locate nearby businesses. Likewise, an application developer may be the *first-party* service provider when it provides a service for turn-by-turn driving directions, regardless of who the underlying wireless carrier might be.[39] CTIA Guidelines require the first party service provider to provide notice and obtain consent. [40]

With respect to COPPA compliance, it would subvert the entire user experience if each Operator interfacing with a website or online service has to obtain opt-in consent at the point of contact with users. Consumers would find it cumbersome and annoying, as well as confusing, to have multiple notices or policies pop-up on a website each time they access the site. Since multiple Operators may be involved, it will be more effective to have the *first-party* Operator seek consent from parents and to make it the responsibility of the *first-party* Operator, not the

[39] CTIA Guidelines at 2.
[40] CTIA Guidelines at 1-2.

parent, to insure that the privacy policy of each Operator is consistent with the privacy notice provided by the *first-party* Operator. Further, to the extent that a third-party service, such as Google Maps,[41] is a "general audience" service available on websites or applications that may or may not be subject to COPPA, it is problematic to assume that the third-party Operator has actual knowledge of a user's age or that the website or application is directed at children.

Similarly, a third-party Operator does not always have actual knowledge as to what information pertaining to children is being collected. For example, an advertiser that distributes ads through an advertising network does not always know which websites and applications are displaying its advertising. A third party that collects data from anonymous cookies may not know that it is collecting information from a device used by a child if the cookie is placed on a general audience website. Likewise, an ad network may interface with multiple websites and may not be aware that some of these websites collect information from children or could be deemed directed to children. This is particularly true since content regularly changes on websites.

Finally, the NPRM raises many questions about the allocation of responsibility for applications that interface with software development kits ("SDKs").[42] For example, if an SDK is made widely available to all mobile application developers and that SDK collects a unique device ID or other identifier, is the SDK platform provider required to provide notice and consent since some applications may happen to be children's games? If so, under what conditions? Does a platform provider have to review every application to ensure compliance

[41] Google Maps, http://maps.google.com/ (last visited Dec. 15, 2011).
[42] As SDKs have become freely available, application publication and downloading have soared. *See* Ingrid Lunden, *Apple's Leagues Ahead in App Downloads: 18 Billion To Android's 10 Billion*, 2011, *available at* http://paidcontent.org/article/419-apples-leagues-ahead-in-app-downloads-18-billion-to-androids-10-billion/ ("Apple says that 500,000 apps have now been published in the App Store, and it has had downloads of 18 billion across the store since it launched three years ago.")

with COPPA? What types of processes would the provider need to create in order to achieve compliance?

To minimize confusion, it is more practical if third parties – such as mobile device manufacturers, carriers, technical support providers, SDK providers, payment networks and advertising networks – are permitted to rely on consent given to first-party Operators. First-party Operators should be permitted to serve as the contact point for all other entities interfacing with their websites, online services or applications. It is logical for the first-party Operator to notify users about the other types of entities that may be using, collecting, or disclosing personal information through the first-party website, online service or application. Indeed, other service providers may not even have knowledge that a website Operator is targeting children or has actual knowledge that it is serving children. At a minimum, a third party should be permitted to rely on the representation of the first-party Operator as to whether or not the website or application is directed to children. If so, the first-party Operator should be permitted to obtain parental consent on behalf of the third party. The third party should be able to rely on such representation to determine whether it should block that first-party Operator from interfacing with the third party's site, service or application. The plain language of the COPPA statute is clear – Congress intended for the first-party *operator* (singular) of a website or online service, not multiple operators, to be bound by the statute's requirements.[43] Congress did not intend to create a chain of liability for all entities that may interface with websites, applications or online services at some point, either now or in the future.

[43] *See, e.g.*, 15 U.S.C. § 6502(a)(1) (2010) ("[i]t is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b) of this section.").

## V. OTHER PROPOSED CHANGES REQUIRE FURTHER FTC EVALUATION AND CLARIFICATION

### A. The Proposed Expansion of the Definition of "Collect or Collection" Requires Clarification

The FTC proposes to broaden the definition of "collect or collection" by adding the terms "prompting" or "encouraging," not just "requesting" a child to provide personal information.[44] The proposed revision also includes, without qualification, "[t]he passive tracking of a child online."[45] As indicated in the ongoing policy and technical discussions about "do not track" functionality in Web browsers,[46] there is no clear consensus regarding what does and does not constitute "tracking." If passive tracking is to be included in the definition, there needs to be clear guidance as to what constitutes "tracking" in the context of the FTC's proposal. If the proposed changes regarding geolocation information and identifiers are adopted,[47] it is unclear whether there can be any data collection online that would not constitute "tracking." Likewise, it is unclear whether the term "passive tracking of a child online" would include tracking a device or if it applies only to a specifically identifiable child. Moreover, the terms "prompting" and "encouraging" remain ambiguous and at the very least should be clarified with specific examples. In any event, the FTC should explain and substantiate why its proposal to expand the coverage of the COPPA regulation to passive tracking is necessary and appropriate, and no more burdensome than necessary, in light of harms or risks that the FTC should expressly identify.

---

[44] Proposed Rule, 76 Fed. Reg. at 59829, § 312.2(a) (*amending "collects* or *collection"*).
[45] *Id.* at § 312.2(c) (*amending "collects* or *collection"*).
[46] *See, e.g.*, Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011).
[47] Proposed Rule, 76 Fed. Reg. at 59830, § 312.2(g)(j) (*amending "personal information"*).

### B. The Proposed Rule Should Be Narrowly Tailored So As Not to Stifle Innovative Cloud Services

Cloud services such as Gmail,[48] Snapfish, iCloud and the Amazon Cloud Drive,[49] as well as sub-contractors of cloud providers, while increasingly prevalent are nonetheless still in the nascent stage. Essentially, "cloud computing is maintaining data, applications, and programs on a remote server that can be accessed through many devices, such as desktop computers, netbooks, or smartphones."[50] When using a cloud service, a person does not have to save data to his or her personal device and can access it through multiple devices. A company like Amazon may offer multiple cloud products such as Amazon Web Services, Elastic Compute Cloud, SimpleDB, CloudFront, and SQS.[51] Other examples include Snapfish, Flickr, Picasa and DropBox.

In order to provide cloud services, multiple entities may be involved even though they are invisible to users. The cloud service provider may engage sub-contractors, agents or vendors, who may technically collect "personal information" under the FTC's proposed definition of the term. For example, these "behind-the-scenes" entities may collect IP addresses or cookie data to enable the primary cloud service to function efficiently and provide the functionality the user wants – namely, secure data storage and easy access to stored data. To allow nascent cloud services and technology to realize their full potential, the proposed rule must be narrowly tailored so that cloud service providers are not directly or indirectly restricted by COPPA requirements if an Operator chooses to use their services.

---

[48] Gmail, http://www.gmail.com (last visited Dec. 15, 2011).
[49] Amazon Cloud Drive, https://www.amazon.com/clouddrive/learnmore (last visited Dec. 15, 2011).
[50] Heidi Salow, Jeremy Meier, and David P. Goodwin, *Cloud Computing Trend Sparks Compliance Concerns*, NATIONAL DEFENSE, (2011), *available at* http://www.gtlaw.com/NewsEvents/Publications/PublishedArticles?find=151061.
[51] Amazon Web Services, http://aws.amazon.com (last visited Dec. 15, 2011).

## VI. THE ELIMINATION OF "EMAIL PLUS" WILL IMPOSE HARDSHIP ON PARENTS, OPERATORS AND SERVICE PROVIDERS

"Email plus," currently permitted under the Rule's sliding scale approach to parental consent,[52] is widely used by Operators and imposes a relatively low burden on parents. While CTIA understands the FTC's concern that many children create fictional email addresses or respond on behalf of their parents,[53] CTIA submits that eliminating "email plus" will only discourage parents and kids from using the websites and online services geared to children.

While there are no fool proof methods of authenticating a user's age and identity, "email plus" has been a reliable and efficient method of authentication. CTIA strongly recommends that the Commission retain "email plus" as a consent mechanism or at a minimum publish empirical studies demonstrating that "email plus" is ineffective or has somehow created harm. The FTC should justify any departure from a methodology that is well established and not unduly burdensome. In addition to "email plus," CTIA and its members will continue to seek alternative methods of authentication that are efficient, reliable and not cumbersome for users, parents and Operators.

## VII. THE PARENTAL NOTICE REQUIREMENTS SHOULD BE CLARIFIED WHEN THERE ARE MULTIPLE OPERATORS

The FTC proposes to change the notice requirement for direct notice to ensure "just-in-time" notice and to streamline the placement and content of online notices.[54] Such changes will have a profound impact on multiple Operators or associated service providers.[55] Websites generally are a complex amalgam of content and services from many different sources. A single website or mobile application may interface with half a dozen different entities. These entities can change quickly and frequently.

---

[52] *Id.* at 59817; 64 Fed. Reg. 59914, § 312.5(b).
[53] This is not a technology issue – children also sign their parent's name on notes to teachers, consent forms, etc.
[54] Proposed Rule, 76 Fed. Reg. at 59815-16.
[55] *See supra* II. B.

The Proposed Rule requires all Operators that collect information from children to provide their contact information on the "home or landing page or screen of its website or online service," and at the point of collection.[56] Thus, where several Operators are interfacing with a single website, the primary Operator and each third-party Operator would have to provide contact information at each place where they collect information from children. The result would be a bewildering and frustrating experience for mobile consumers. It also would confuse parents about which of these multiple entities to contact with a question or concern. Such a result is clearly not what Congress intended when it passed COPPA.[57]

In the NPRM, the FTC cites a mobile application and its corresponding advertising network as an example of multiple Operators at work on a single online service.[58] It is easy to understand that when multiple entities are collecting personal information directly from users actually known to be children for their own purposes, they each have an independent obligation to comply.[59] Compliance obligations becomes murky when the collection is automatic or passive, or in a context where neither Operator has actual knowledge that a user is a child, or where one Operator offers a general audience service and the other offers a service directed towards children. Thus, with multiple Operators, it is not clear under the proposed rules which Operator must provide notice and obtain consent to avoid COPPA liability. It becomes even more complicated in the open model of the mobile environment where general audience services allow other services to integrate within their platforms or to be integrated into another services platform. Flurry, for example, interfaces with multiple third parties to provide its mobile application analytics services, and it mandates that its customers not use the Flurry services in

[56] Proposed Rule, 76 Fed. Reg. at 59830, § 312.4(b).
[57] *See* 64 Fed. Reg. at 59894 nn.91 & 92 (specifying that an Operator's notice should be clear, understandably written, complete, and have no confusing information).
[58] Proposed Rule, 76 Fed. Reg. at 59815.
[59] In this instance, the COPPA Rule would not even need to be amended.

connection with any application or service directed toward children or collect personal information of children.[60]

The FTC's proposed notice requirements raise many issues that the Commission must address before it adopts its Final Rule. Specifically, is the mere association of a general audience website/online service with a website/online service governed by COPPA enough to trigger liability for failure to notify? What types of arrangements trigger liability by association? Whether and under what circumstances is an online store that offers the ability to purchase or download third party content directed toward kids (games, videos, music, etc.) liable for failure to provide direct notice to parents?

If the consent process is too onerous, it could stifle innovation, directly conflicting with the goals of the Proposed Rule.[61] And if users are continually bombarded with multiple policies to read, the user experience will suffer and entities may stop providing services to websites. To address some of these issues, CTIA urges the Commission to reevaluate its proposals with respect to notice requirements and multiple Operators and designate the first-party Operator as the appropriate entity to provide notice and serve as the point of contact. This will alleviate confusion and provide a more straightforward approach for consumers and Operators. Also, general audience online service providers who openly provide integrations or a marketplace to multiple developers and who do not wish to associate with developers who direct content to children or collect information from children, should be able to continue to openly allow integrations with prohibitions on these sorts of activities or require developers who engage in such activities adhere to COPPA if applicable.

[60] Flurry Privacy Policy, http://www.flurry.com/about-us/legal/privacy.html (last visited Dec. 15, 2011).
[61] Proposed Rule, 76 Fed. Reg. at 59804.

## VIII. VERIFIABLE PARENTAL CONSENT

While CTIA fully supports the use of verifiable parental consent, the Commission's proposed new methods to obtain verifiable parental consent – including electronic scans of signed parental consent forms, video-conferencing, and government-issued identification checked against a database[62] – are far more burdensome for both parents and Operators. Many parents do not have video conferencing ability, nor do they own scanners.

In addition, Operators would have to collect a considerable amount of additional personal information from parents that they do not currently collect under the existing COPPA rules. After parents provide this information, it is not simply a matter of hitting the "delete" button since Operators would have to maintain logs to prove parental consent to resolve disputes. Furthermore, the information may remain in stored backup copies.

CTIA and its members continue to explore additional methods to obtain verifiable parental consent, and hope that the Commission will continue to consider new options.[64]

## IX. SMS AND MMS TEXT MESSAGES ARE NOT COVERED BY COPPA'S TERMS

SMS and Multimedia Messaging Service ("MMS") text messages are not covered by COPPA because they do not use the public Internet or DNS addresses.[65] CTIA supports the

---

[62] Proposed Rule, 76 Fed. Reg. at 59831 § 312.5(b)(2). The creation of such a public database actually creates the very problem that the FTC is attempting to solve by making PII available in a centralized and easily accessed database for hackers and misuse. *See* Thierer, Adam D. *National ID Cards: New Technologies, Same Bad Idea* (Sept. 28, 2001), http://www.cato.org/pub_display.php?pub_id=11552 (last visited Dec. 22, 2011). *See also* Thierer, Adam D. *Kids, Privacy, Free Speech & The Internet: Finding the Right Balance* (Aug. 2011), http://mercatus.org/sites/default/files/publication/Kids_Privacy_Free_Speech_and_the_Internet_Thierer_WP32.pdf (last visited Dec. 22, 2011).

[64] One of the stated purposes of the Proposed Rule is to ensure that COPPA continues to meet its goals as online technologies evolve. 76 Fed. Reg. at 59804.

[65] 15 U.S.C. § 6502(a)(1); *see id.* at § 6501(6).

FTC's correct interpretation of the statute that SMS and MMS text messages that do not travel on a public packet-switched network are not covered by COPPA.[66]

## X. CONCLUSION

Technological advancements have forever changed the myriad ways children access and use the Internet, even in the short time since COPPA was enacted in 1999. With the emergence of wireless Internet access, cloud services and the simultaneous emergence of new types of mobile devices, countless new opportunities for children to access a variety of content, *including age-appropriate educational and entertainment content*, abound. Wireless devices offer new methods of delivering such content, and utilizing data, as well as convenience and safety.[67] To the extent that wireless services such as geolocation services and mobile applications raise privacy concerns, these concerns have been, and will continue to be addressed through industry self-regulatory efforts as well as through appropriate FCC and FTC oversight. Industry initiatives – such as the CTIA Guidelines, the Digital Advertising Alliance ("DAA") Self-Regulatory Principles for Online Behavioral Advertising, the DAA Self-Regulatory Principles for Multi-Site Data and the Mobile Marketing Association's Mobile Application Privacy Guidelines – not only protect the privacy rights that COPPA addresses, they supplement COPPA's protections by placing restrictions on the use of inappropriate content and sharing of certain types of data. The wireless industry in particular has demonstrated its commitment to providing parents with the tools they need to control their children's use of wireless devices.[68]

---

[66] CTIA Comments, *In the Matter of Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Act Rule*, COPPA Rule Review P104503, June 30, 2010, *available at* http://files.ctia.org/pdf/filings/100630_-_FILED_CTIA_COPPA_comments.pdf.

[67] For example, during Hurricane Katrina, emergency workers used smart phones and handheld devices to communicate with each other and people who needed help. Darrell M. West, Vice President and Director, Governance Studies, The Brookings Institution, *Ten Facts about Mobile Broadband*, Dec. 8, 2011, *available at* http://www.brookings.edu/papers/2011/1208_mobile_broadband_west.aspx.

[68] *See* CTIA's & The Wireless Foundation's "Be Smart. Be Fair. Be Safe. Responsible Wireless Use" Campaign at http://www.besmartwireless.com/; AT&T Wireless Parental Controls at http://www.att.net/smartcontrols-

As explained above, CTIA is concerned about several of the FTC's proposed changes to the COPPA Rule. Any such changes must not exceed the Commission's statutory authority and must avoid the unintended consequences described herein. In addition, some of the proposed changes require clarification or should be reevaluated so they do not stifle nascent technological and product innovations. CTIA continues to support the text messaging exemption. CTIA also supports Safe Harbor programs that are not burdensome to adopt, which will encourage wider participation.

We feel our concerns warrant further evaluation and discussion before the Commission can proceed with finalizing the Proposed Rule. CTIA looks forward to an open and constructive dialogue with the Commission about its proposed changes to the COPPA Rule. CTIA also strongly recommends that the Commission use a cooperative, multi-stakeholder process similar to the approach embraced by the Department of Commerce's Internet Policy Task Force, *i.e.*, written and verbal consultations with stakeholders in industry, civil society, academia, and government,[69] with respect to addressing concerns and proposals raised during this phase of the proceeding. CTIA is certain such discussions will be mutually beneficial. Moreover, they are crucial in developing important, well-balanced Internet policy.

**[Balance of page intentionally left blank]**

---

WirelessParentalControls; Microsoft Family Safety Center at http://www.microsoft.com/security/family-safety/childsafety-steps.aspx; Sprint 4netsafety Program at http://www.sprint.com/4netsafety/ and Sprint Safety & Control Services at http://shop.sprint.com/mysprint/services_solutions/category.jsp?catId=service_safety_control&catName=Safety%20and%20Control; T-Mobile Family Allowances and Webguard at http://www.t-mobile.com/shop/addons/services/information.aspx?PAsset=FamilyWireless&tp=Svc_Tab_FW101FamilyAllowances; and Verizon Wireless Parental Controls Center at http://parentalcontrolcenter.com/.

[69] The Department of Commerce published a Privacy and Innovation Notice of Inquiry, invited participation in a Privacy and Innovation Symposium, and ultimately published a green paper entitled "*Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*" in December 2010.

Respectfully submitted,

By: _____

Heidi Salow
Amanda Katzenstein
**GREENBERG TRAURIG, LLP**
1750 Tysons Boulevard, Suite 1200
McLean, VA 22102

2101 L Street, N.W., Suite 1000
Washington, D.C. 20037

**Counsel for CTIA - The Wireless Association®**

Andrea Williams
Vice President of Law & Assistant General Counsel

Michael F. Altschul
Senior Vice President & General Counsel

**CTIA – The Wireless Association®**
*Expanding the Wireless Frontier™*
1400 16th Street, NW, Suite 600
Washington, DC 20036

Dated: December 23, 2011

*TCO 359,400,954v20*