BSA®
BUSINESS SOFTWARE ALLIANCE

Robert W. Holleyman, II
President and Chief Executive Officer

September 24, 2012

The Honorable Donald S. Clark
Secretary
Federal Trade Commission
Office of the Secretary, Room H-113 (Annex E)
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Re: COPPA Rule Review, 16 CFR Part 312, Project No. P104503

Dear Secretary Clark:

The Business Software Alliance (BSA) is an association of the world's leading software and hardware technology companies. On behalf of its members, BSA promotes policies that foster innovation, growth, and a competitive marketplace for commercial software and related technologies.[1] BSA supports the goals of the Children's Online Privacy Protection Act (COPPA) and commends the Commission's attendant focus on protecting children online through its COPPA Rule (the Rule). BSA appreciates the opportunity to comment on the Commission's Supplemental Notice of Proposed Rulemaking (Supplemental NPRM).

BSA respectfully submits that several of the Commission's proposed Rule revisions set forth in the Supplemental NPRM go beyond the scope of the plain language of COPPA, especially in that they would create secondary liability through regulation in a statute that does not contemplate such forms of liability. Further, the proposed revisions would handicap innovation without any attendant benefits for children's privacy.

Specifically, BSA believes the Commission improperly concludes that because an online service provider may benefit in some way – the hallmark of all commercial arrangements – from the actions of other entities that collect personal information from children under 13, that the online service provider should be considered an "operator" under the Rule. We also believe that expanding the concepts of either specifically targeting children under 13 or having actual knowledge of the collection of personal information to add a "reason to know" standard about such collection exceeds the plain language of the statute and is too vague to provide meaningful guidance.

In addition, we urge the Commission to reconsider its proposed, expanded definition of "personal information," which includes "persistent identifiers" not tied to individually identifiable information. We see this expanded definition as

[1] BSA's members include: Adobe, Apple, Autodesk, AVEVA, AVG, Bentley Systems, CA Technologies, CNC/Mastercam, Intel, Intuit, McAfee, Microsoft, Minitab, Progress Software, PTC, Quest Software, Rosetta Stone, Siemens PLM, Sybase, Symantec, and The MathWorks.

exceeding the scope of the statute, and we fear that it would result in the stifling of innovation and beneficial content for users by fundamentally restricting many activities that underlie the efficient functioning of the Internet – including ad serving, attribution, and analytics.

I. The Proposed Definition of "Operator" is Contrary to the Statute.

Absent clarification, the Commission's proposed revisions to the definition of "operator" could result in unjustifiable outcomes, including COPPA liability for entities that clearly are not responsible for the collection of personal information from children under 13. Under the current Rule, "operators" of websites or online services directed to children (*i.e.*, websites or online services that target children) and those having "actual knowledge" of the collection of personal information from children under 13 must comply with the Rule, including notice and parental consent provisions.[2] Operators are entities that operate websites or online services that collect personal information as well as entities "on whose behalf such information is collected or maintained."[3]

The Commission proposes to expand the Rule such that the category of websites and online services that are "directed to children" would include a) those likely to attract children and b) those that "know[] or ha[ve] reason to know" they are collecting personal information from children under 13. The "knows or has reason to know" standard is based on the website or online service likely being attractive to the age group. Whether an operator would be attractive to children under 13 would depend on whether the age group is the primary audience or the operator attracting a disproportionately larger percentage of that age group.[4] The Commission also proposes to add that "personal information is collected on behalf of an operator where it is collected in the interest of, as a representative of, or for the benefit of the operator."[5] These proposals unduly expand the scope of COPPA.

A. *The proposed expansion of activity that renders an entity an operator because information is collected "on behalf of" the entity is far too broad.*

The Commission's proposed Rule could have the unintended consequence of expanding the scope of the Rule to entities that do not collect or have access to personal information from children, but who might have a commercial relationship with a website or online service that does. Until now, the Commission and the Rule have embraced the concept that an entity that lacks

---

[2] 16 C.F.R. § 312.3.
[3] *Id.* at 312.2.
[4] 77 Fed. Reg. 46,643, 46,646 (Aug. 6, 2012) (proposed 16 C.F.R. § 312.2).
[5] *Id.* at 46,645 (proposed 16 C.F.R. § 312.2).

access to or control over personal information is not an operator.[6] The Commission's proposal relating to entities that act on behalf of another operator could be read to sweep in entities far removed from the actual collection of personal information from children under 13.

We believe the Commission's focus on an "interest" or "benefit" rendering another entity an operator goes too far. For example, the Commission proposes that plug-ins and applications could be operators in their own right. Accordingly, under the Commission's proposed approach, application platform providers, such as mobile phones, e-readers, tablets and associated app stores, despite being removed from the consumers' direct interaction with a particular application (or "app") could nonetheless be liable under the proposed revisions to the Rule for violations by an app offered on the platform. The platform provider, even though it may not collect any personal information, may be attractive to children who want to download certain apps. Where an app is attractive to children or knowingly collects personal information from children under 13 based on the downloading and use of the app, the platform provider, as a function of its commercial relationship with an app developer, even though it does not collect personal information from the child, might receive some benefit from the app being downloaded from its platform.

The Commission should rethink its proposal because an entity that benefits in any way from the application – in our example the platform provider who is not collecting information from the child – could be deemed to be acting "on behalf of" the application. The Commission explains that where a child-directed online service integrates and offers apps that collect personal information from a child, the personal information is collected on the service's (i.e., the platform's) behalf even though the platform "does not own, control, or have access to the information collected."[7] Congress could not have intended such an attenuated result.

In a commercial context, each party to a relationship obtains some benefit from the others. Yet every party benefitting from a commercial transaction clearly is not acting *on behalf of* the others. It would be one thing if apps acted as "agents" of or "as a representative of" the platform provider, but they do not. The platform simply makes available other, independent services that consumers interact with directly. As between an app and a platform provider, the app collects information on its own behalf, not on behalf of the application's platform.

---

[6] 64 Fed. Reg. 22,750, 22,752 (Apr. 27, 1999) ("Where the website or online service merely acts as the conduit through which the personal information collected flows to another person or to another person's website or online service, and the website or online service does not have access to the information, then it is not an operator under the proposed Rule."); *See* 64 Fed. Reg. 59,891 (Nov. 3, 1999) (affirming this view).

[7] 77 Fed. Reg. at 46,644.

Moreover, we think that the Commission's proposal is inconsistent with the overall structure of COPPA and the Rule. Under COPPA, operators must provide notice of use and obtain consent for use of personal information of children under 13 and provide the personal information to parents upon request. Where an entity has no relationship to the collection and use of the personal information, it makes no sense to hold that entity accountable for any violations related to notice, consent or parental access. The lack of some entities' ability to address these aspects of COPPA further bolsters the argument that the collection of information was not on behalf of those entities.

B. The addition of a "reason to know" standard sweeps too broadly.

In addition to the unduly sweeping breadth of entities that might be deemed operators based on the Commission's proposal related to entities that operate on another's behalf, we believe the Commission's proposed "reason to know" standard suffers from similar flaws. First, in the context of the discussion above relating to a platform provider's potential to be deemed an operator, a platform provider having a "reason to know" that apps it offers target or are attractive to children and collect personal information from children should not subject the platform provider to COPPA. This analysis should be the same if the platform had actual knowledge of such collection. The app does not act on behalf of the platform in either circumstance.

Second, COPPA itself specifies the standard for when COPPA would apply to an operator: when an operator maintains a website or online service that is "directed to children" or where the operator has "actual knowledge that it is collecting personal information from a child."[8] Accordingly, the proposed revisions to the Rule go too far in cases where third-party apps, plug-ins, ad networks, and other services that are used in conjunction with a website or other service are not independently directed toward children and lack actual knowledge of the collection of information from children under 13. Apart from the platform issue discussed above, third-party services such as apps, plug-ins, and advertising networks frequently have very little control over where or how they are used in conjunction with first-party services that have direct relationships with users. In the complex and ever-shifting ecosystem of the web, liability based on an amorphous "reason to know" standard would stifle innovation and opportunities for children and others to benefit from services and online tools.

Finally, these provisions, whether applied to platform providers, apps, plug-ins, or advertising networks, could result in third-party entities that do not have direct relationships with users from whom data is collected being held liable for COPPA violations. There is no evidence that Congress intended to create a scheme of liability for entities that are acting as mere agents or processors on

---

[8] 15 U.S.C. § 6502(a)(1).

behalf of a website or online service that itself collects personal information from children or that purposefully enables entities acting as its agent to collect such information. Where a third party "knowingly" collects personal information from children on its own behalf or uses agents to do so, that third party would appropriately be covered by COPPA, a law which – through its use of the words "directed" and "targeted" – focuses on operators' intent. Absent any such intent by a third party to collect personal information from children under 13 or actual knowledge of such collection, however, creating a secondary liability scheme falls far outside the statutory bounds of COPPA.[9]

II. The Proposed Definition of "Personal Information" is Inconsistent with the Plain Language of the Statute and Far Too Broad.

The statutory definition of "personal information" under COPPA requires "individually identifiable information."[10] As such, we believe that the Commission's approach to persistent identifiers that do not themselves individually identity an individual exceeds the scope of the statute. Moreover, the Commission fails to recognize that cross-website activities involving persistent identifiers still benefit and are integral to the internal operations of a website or online service in its carve out for activities that support internal operations.

A. The statute does not support the Commission's proposed interpretation.

The Commission's proposals to expand the definition of "personal information" circumvent the plain language of the COPPA statute, and therefore these proposals would be unlawful if finalized. COPPA 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***.[11]

The Commission's treatment of persistent identifiers in the current Rule comports wholly with the statute, focusing on whether the persistent identifier (like a customer number held in a cookie) "is associated with individually identifiable information; or a combination of a last name or

---

[9] If the Commission seeks to impose some type of secondary liability on various parties, it should at least provide some type of "safe harbor" to entities, such as platforms, websites, plug-ins and apps that act in a responsible manner.

[10] 15 U.S.C. § 6501(8).

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

photograph of the individual with other information such that the combination permits physical or online contacting." [12]

Under the Commission's proposed Rule, personal information includes a "persistent identifier that can be used to recognize a user over time, or across different Web sites or online services [excluding internal operations ... and] includes but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier." [13] In its proposed revisions to the Rule, the Commission misread the statute in viewing the use of these persistent identifiers as being equivalent to the use of personal information.

In our view the Commission has misread the COPPA statute by assuming a cookie, IP address or other identifier could be used to "contact" a specific individual. The prefatory language in the COPPA statute that relates to contacting a specific individual requires first that the personal information be "personally identifiable information." This presupposes that an operator must be able to contact a "specific individual," which requires that the operator be able to identify a specific individual. Anonymous activity, such as serving an advertisement to an "unknown" or "unnamed" person that happens to be using a specific IP address is not covered by the language in the statute.

BSA understands that persistent identifiers, if combined with other persistent identifiers or with other personal information, might result in individually identifiable information and the contacting of a specific individual. But, absent any specific additional steps by an operator to specifically identify an individual, we believe the Commission is without authority to adopt its expanded definition of personal information.

B. The proposal does not appear to allow common, non-privacy-invasive activities.

While the Commission's Supplemental NPRM clarifies the scope of the exception allowing the collection of persistent identifiers that are used as "support for the internal operations of the website or online service," it does so too restrictively. First, as noted above, any restriction on the collection of persistent identifiers should be limited to persistent identifiers that contain or are combined with individually identifiable information. But if there is a "support for the internal operations" exception, it should not be limited to the enumerated purposes, including contextual advertising. Various activities based on the use of persistent identifiers across websites benefit users and enable a more efficient Internet with more valuable content. Even if the Commission were to restrict the delivery of advertising targeted to children based on information collected

[12] 16 C.F.R. § 312.2.
[13] 77 Fed. Reg. at 46,652 (proposed 16 C.F.R. § 312.2).

through persistent identifiers across websites (which in BSA's view still goes too far) there are many consumer beneficial activities that the collection and use of persistent identifiers across websites enable, including the serving of contextual advertising, ad tracking, and conducting advertising analytics.

An ad network or ad server can use a persistent identifier across websites in a manner that does not involve the delivery of behavioral ads based on multi-site user activity. The ad network can aggregate the individually logged data, prepare reports about how many unique users saw the ads, which ad or site brought traffic to the advertiser during the next month, and which ads drove specific actions at the advertiser site. Such activity does not have to entail the creation of profiles or behavioral advertising, but it can involve the anonymous tracking of actual individuals for analytics and ad reporting purposes. These functions provide vital contributions to the efficient operation of a website (and the Internet generally) and ultimately benefit all Internet users, including children.

* * *

For the reasons above, BSA respectfully requests that the Commission reassess its approach consistent with the confines of the COPPA statute and the practical ramifications of its proposed changes, which would negatively impact the efficient operation of the Internet and the services available to users.

Sincerely,

Robert W. Holleyman, II
President and CEO