Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

December 21, 2011

VIA ELECTRONIC FILING

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

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

Dear Secretary Clark:

Microsoft welcomes the opportunity to provide these comments on the Commission's proposed revisions to its rule implementing the Children's Online Privacy Protection Act ("COPPA").[1] We commend the Commission for carefully considering the record compiled to date in response to the 2010 request for public comment. As explained in our June 2010 comments to the Commission[2] and in our testimony before Congress,[3] Microsoft has a deep and long-standing commitment to protecting the privacy of consumers, including children, who use our websites and online services. And we believe that COPPA and the COPPA Rule can play an important role in encouraging parental involvement and protecting children's privacy and safety online.

We appreciate that the Commission's proposed revisions to its COPPA Rule attempt to achieve several objectives, including to provide meaningful privacy protections for children,

[1] 15 U.S.C. §§ 6501-6508.

[2] Letter from Michael D. Hintze, Associate General Counsel, Microsoft Corporation, to Mr. Donald S. Clark, Secretary, Federal Trade Commission (June 30, 2010), *available at* http://www.ftc.gov/os/comments/copparulerev2010/547597-00038-54848.pdf [hereinafter, "Microsoft 2010 Comments"].

[3] Statement of Michael D. Hintze, Associate General Counsel, Microsoft Corporation, Before the Senate Commerce, Science, and Transportation Subcommittee on Consumer Protection, Product Safety, and Insurance, "An Examination of Children's Privacy: New Technologies and the Children's Online Privacy Protection Act" (Apr. 29, 2010), http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=938c8dd3-4912-4ff9-9286-a4805710fb2d&Statement_id=d557118e-8d99-42ca-8647-082584333c0d.

ensure that the Rule keeps pace with evolving technologies and Internet practices, and provide industry with practical guidance.

In a number of important respects, the Commission's proposed rule advances these objectives. For example, Microsoft is encouraged by the fact that the Commission seems open to expanding its list of approved parental consent mechanisms. As we explained in our June 2010 comments on the Commission's COPPA Rule review, today's technologies and the realities of Internet use require the approval of new methods for parental verification and consent that are more parent-friendly, pragmatic and simple, and that scale for popular services.[4]

Microsoft agrees with the Commission that COPPA should not be amended to replace the "actual knowledge" standard with a broader "constructive knowledge" or similar standard. The Commission appropriately recognizes that the actual knowledge standard "is far more workable, and provides greater certainty, than other legal standards that might be applied to the universe of general audience Web sites and online services."[5] As described in more detail below, applying a "constructive knowledge" or similar standard would be especially problematic where website operators rely on ad networks and other third-party online service providers to, for example, display advertising and deliver content, applications, and other interactive online services to users, because these third parties are not in a position to independently investigate or determine whether a particular user is a child.

In addition, Microsoft supports the Commission's conclusion that 13 years remains an appropriate age threshold for defining when a user is a "child" under COPPA. It certainly is true that COPPA's goals of increasing parental involvement and protecting privacy are important with respect to teenagers. But the Commission is correct that COPPA's existing structure and parental consent processes are not well suited to deal with this age group. In addition, teen use of the Internet raises different privacy and safety issues as compared with those typically raised for children under 13. To help protect teen privacy and safety online, Microsoft provides parents with a number of educational resources and technology tools so that they can talk to their teens about these issues.[6]

Finally, we are pleased to see a number of clarifications that address current ambiguities in the Rule and that will provide greater certainty for companies and parents going forward.

There are some proposed changes, however, where it is unclear how the revised COPPA Rule would apply in practice or would effectively address the concerns the Commission raised. In these circumstances, greater certainty and more practical guidance is needed for consumers and industry.

---

[4] Microsoft 2010 Comments, at 9.

[5] 76 Fed. Reg. 59804, 59806 (Sept. 27, 2011).

[6] *See, e.g.*, http://www.microsoft.com/security/family-safety/childsafety-age.aspx; http://go.microsoft.com/?linkid=9787289; http://www.microsoft.com/security/resources/book-teens.aspx.

Specifically, Microsoft encourages the Commission to:

- Provide greater clarity on the meaning of "tracking" as used in the COPPA Rule's definition of "collects or collection;"

- Move cautiously in expanding COPPA's scope to include persistent identifiers, on their own, as "personal information," or, at a minimum, further clarify the COPPA Rule to minimize the potential for unintended consequences of such a broad expansion of the Rule's scope;

- Add provisions clarifying the obligations and liabilities of different parties where third-party online service providers collect persistent identifiers or other personal information through a first-party website, application, online gaming platform, or other online service;

- Recognize that third-party geolocation services present many of the same challenges as other third-party online services and, accordingly, streamline the COPPA Rule's requirements for providers of third-party geolocation services as well;

- Streamline the parental notice and consent requirements in cases where there are multiple operators in order to prevent imposing undue burdens on parents;

- Clarify that an operator will not be deemed to gain actual knowledge from photograph, video, or audio files that contain information that merely may suggest that a particular user is under 13 years old; and

- Expand the definition of "support for the internal operations of the Web site or online service" to explicitly include activities that are necessary to improve the website or online service as well as those that are necessary for the functioning of the website or online service.

The further clarifications and revisions to the COPPA Rule identified above and described in further detail in these comments will provide industry with clearer, more practical guidance about how the COPPA Rule applies to new technologies and business practices that have emerged since COPPA was enacted over ten years ago, while still ensuring that children's privacy and safety are protected online, encouraging parental involvement in children's online activities, and enabling children to continue to have access to online services.

I. The Commission Should Define What Constitutes "Tracking" for Purposes of the COPPA Rule's Definition of "Collects or Collection."

COPPA's requirements are triggered when an operator of a website or online service "collects" personal information from a child online and either directs the website or service to children under 13 or has actual knowledge that the user is a child. Under the current COPPA

Rule, "collects or collection" is defined to include the "passive tracking or use of any identifying code linked to an individual, such as a cookie."[7] The Commission proposes to revise this definition to cover, without qualification, the "[p]assive tracking of a child online." In its request for comment, the Commission states that this change is intended to simplify the definition and to "clarify that [the definition] includes all means of passive tracking of a child online, irrespective of the technology used."[8] However, because there is disagreement about what the term "tracking" means in the broader online environment, the revision, while well intentioned, could create additional uncertainty.

In the broader discussion of "do not track" functionality for web browsers, no clear consensus has emerged on what constitutes "tracking" or what it means not to "track" an individual or a device. Some have suggested that "tracking" occurs whenever data is collected. Others recognize that there are a number of legitimate reasons for collecting data — such as analyzing website traffic patterns and storing online passwords — and therefore suggest that "tracking" should be defined narrowly to include only certain data uses.[9] Some browsers have addressed this issue simply by adding a "do-not-track" signal in the header information sent to a website,[10] but there is not yet any consensus about what a website or online service should do, or refrain from doing, in response to that signal.

The meaning of "tracking" in the context of COPPA is critical because the revised COPPA Rule proposes to expand the definition of "personal information" to include screen names, user names, and all forms of persistent identifiers, when used for certain purposes. Absent clarification, it is not clear whether there can be any data collection online by ad networks and other third-party online service providers that would not constitute "tracking." Such an expansive interpretation of what constitutes a "collection" of personal information for purposes of COPPA could unwittingly discourage websites from offering innovative content, applications, and interactive online services to children.[11]

---

[7] 16 C.F.R. § 312.2.

[8] 76 Fed. Reg. 59804, 59808 (Sept. 27, 2011).

[9] *See, e.g.*, Julia Angwin & Jennifer Valentino-Devries, "FTC Backs Do-Not-Track System for Web," WALL STREET JOURNAL (Dec. 2, 2010), http://online.wsj.com/article/SB10001424052748704594804575648670826747094.html.

[10] Microsoft has taken a more robust approach, introducing its "Tracking Protection" feature in Internet Explorer 9, which allows consumers to decide which third-party sites can receive their data and filters content from third-party sites identified as potential privacy threats. By limiting "calls" to third-party websites, Internet Explorer 9 blocks these third-party sites from collecting information from users – without relying on these third-party sites to read, interpret, and honor a do-not-track signal. *See* http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/features/tracking-protection.

[11] As an example, Flurry, a popular analytics and monetization platform for mobile applications, recently announced that it will not permit its services to be used on any applications that are directed to children or collect personal information from children. See http://blog.privacychoice.org/2011/10/25/developer-alert-flurry-analytics-adopts-new-child-privacy-rule/. If other third-party service providers, including ad networks, take similar

To avoid this result, we encourage the Commission to provide clear guidance on what specific activities constitute "tracking" for purposes of COPPA. Specifically, we suggest that "tracking" be limited to the creation of a behavioral profile of a child based on the collection of information about the behavior of that child across unrelated websites or online services. Thus, merely serving advertisements across multiple websites by a third-party ad network (which inherently involves some logging of page views in association with an IP address and/or a cookie ID) would not constitute "tracking" unless the ad network uses that logged data to create a behavioral profile of the user. Such a rule would permit an ad network to deliver non-behaviorally-targeted advertisements on websites directed to children (or to a user known to be a child). This approach should not constitute "tracking" because such activity presents minimal privacy risks, while enabling operators to provide free, advertising-supported content and services directly to children.

II. The Commission Should Move Cautiously with Any Expansion of COPPA's Scope with Respect to Persistent Identifiers, or, at a Minimum, Further Clarify the COPPA Rule To Minimize Additional Burdens on Parents and Companies.

Currently, a persistent identifier, such as an IP address or cookie ID, is not "personal information," as that term is defined by the Rule, unless it is associated with individually identifiable information.[12] The revised Rule takes a different approach, deeming a persistent identifier, on its own, to be "personal information," except to the extent it is used to support the internal operations of the website or online service.[13]

The decision to expand COPPA's scope to more broadly encompass persistent identifiers appears to be aimed largely at restricting online behavioral advertising targeted at children.[14] Microsoft agrees with the Commission that advertising to children raises important policy issues. Indeed, Microsoft goes beyond the COPPA Rule's current requirements and has made a policy decision not to behaviorally target advertising to users whom it knows are under the age of 13. Further, we believe that COPPA can play an important role in protecting children's privacy in this context.

However, the proposed revisions, by broadly expanding the scope of COPPA, may lead to a number of unintended consequences that could undermine the well-intentioned objectives of the Commission. Specifically, as explained below, the proposed changes could create marketplace uncertainty for ad networks and other third-party service providers that offer

---

steps to protect themselves from liability under COPPA, the economic basis for child-directed websites, applications, and online services could be significantly weakened.

[12] 16 C.F.R. § 312.2.

[13] 76 Fed. Reg. 59804, 59811 (Sept. 27, 2011).

[14] *See id.* at 59811–12 ("However, the new language would require parental notification and consent prior to the collection of persistent identifiers where they are used for purposes such as amassing data on a child's online activities or behaviorally targeting advertising to the child.").

content, applications, geolocation services, or online services through first-party websites and platforms. The change could also have the effect of reducing incentives to use anonymization and de-identification techniques that help protect children's privacy online. Finally, the revised COPPA Rule, if enacted, could inadvertently create unnecessary costs and doubt for consumers, industry, and regulators because the Rule may be subject to challenge on the basis that the statute does not give the Commission the clear authority necessary to expand COPPA's scope in the manner proposed.

If, notwithstanding these concerns, the Commission decides to expand COPPA's scope to more broadly cover persistent identifiers as "personal information," Microsoft encourages the Commission to clarify the Rule to minimize areas of uncertainty and to focus the COPPA Rule (and not just the definition of "personal information") on data uses, rather than on data collection.

A. <u>The Proposed COPPA Rule Revisions May Cause Significant Marketplace Uncertainty for Ad Networks and Other Third-Party Online Service Providers.</u>

As explained in our June 2010 comments on the Commission's COPPA Rule review, Microsoft believes that the COPPA Rule is broad enough to cover a number of online advertising scenarios where the operator collects, uses, or discloses children's personal information online.[15] However, to the extent the proposed COPPA Rule revisions are intended to more fully capture and restrict online behavioral advertising activities, the revisions may not fully achieve this objective and instead are very likely to create significant marketplace uncertainty.

As the COPPA statute is drafted, an ad network or similar third party is subject to COPPA only if it (1) operates a website or online service directed to children or (2) has actual knowledge that it is collecting personal information from a child.[16] Microsoft is not aware of any ad network that is "directed to children," and an ad network typically is not in a position to obtain "actual knowledge" of a consumer's age. Consequently, capturing the activities of a typical ad network would require strained statutory interpretations that implicitly introduce a "constructive knowledge" standard into the COPPA framework and that have the effect of causing significant marketplace confusion.

For instance, ad networks could be captured by the revised COPPA Rule if the Commission concludes that a third-party ad network has "actual knowledge" that the user is a child when it displays an ad on a website that is arguably directed to children. However, this interpretation improperly conflates the "directed to children" and "actual knowledge" standards.[17] This interpretation also implicitly introduces a "constructive knowledge" standard,

[15] Microsoft 2010 Comments, at 9.

[16] *See, e.g.*, 15 U.S.C. § 6502; 16 C.F.R. § 312.3.

[17] The "directed to children" standard and the "actual knowledge" standard are two distinct standards. It should not be the case that an operator has "actual knowledge" simply because a user once visited a site "directed to

because ad networks that direct their services to a general audience would be deemed to have knowledge of age based purely on circumstantial factors, such as the nature of the site where the advertising is displayed.

Such an interpretation also would be overly broad, thereby creating significant uncertainty in the marketplace. Suppose, for example, that an ad network delivers ads to a device that visits 20 different websites — one of which arguably is directed to children under 13 and 19 of which are clearly directed to a general audience. The weight of the evidence in such a scenario is that the user (assuming there is only one user) of the device is not a child. This conclusion is supported by the fact that many adults have, at one time or another, visited a site that is arguably directed to children, perhaps because they are interested in the particular brand or because they want to evaluate whether to allow their children to register on or visit the site. If ad networks are required to treat any device that visits a website that arguably is directed to children as belonging to a child under 13 years old, then nearly every device could be deemed to be the device of a child. Ad networks either would be forced to bear unnecessary costs to comply with COPPA's requirements for all of these users, many of whom would be 13 years old or older, or be left with very few users to whom targeted ads could be shown. This result would have profound implications for online advertising and major economic impacts across the Internet – including the thousands of general audience websites that rely on online advertising to support their content offerings and services.

Alternatively, ad networks could be captured by the revised COPPA Rule if the Commission concludes that a third-party ad network is "directed to children" if it displays an ad on a website that is directed to children. This interpretation, however, leads to the same impractical results. It would likewise indirectly introduce a "constructive knowledge" standard into the COPPA Rule, because this determination would be based on the nature of the website where the advertising is displayed and over which the third-party ad network has no control and, in many cases, no direct insight.

In either example, the ad network would be placed in the impossible position of determining whether or not any of the websites where it displays ads are "directed to children." Even if an ad network were able to review the content of these sites, over which it has no control, its evaluation would be incomplete because the Commission considers a number of factors that have nothing to do with the website's content when determining whether a website or online service is directed to children, including competent and reliable empirical evidence regarding the intended audience. The ad network also would need to regularly re-evaluate every page of each website to make sure the content had not changed since its last review in a way that would make it more likely to be deemed directed to children. Given that ad networks serve ads on millions of pages and thousands of websites, this burden cannot realistically be met.

---

children." That would make the "directed to children" prong merely a subset of the "actual knowledge" prong. That is not how Congress drafted the statute, and that is not a result that could be practically applied.

The Commission can avoid these results and reduce the likelihood of uncertainty by clarifying the Rule as suggested below in Section II.D.

B. Treating Persistent Identifiers the Same As Information That Directly Identifies an Individual Could Discourage Operators from Using Anonymization or De-Identification To Protect Children's Privacy Online.

Despite research calling some anonymization and de-identification methods into question,[18] many techniques for replacing personally identifiable information with an anonymized or de-identified persistent identifier can still be a very effective means for reducing risk and helping to protect the privacy and safety of individuals online – including children. Anonymization and de-identification methods come in various strengths and have a spectrum of uses ranging from general risk mitigation to securing highly sensitive information. For example, for users who have created Windows Live accounts, rather than using the account ID as the basis for our ad systems, Microsoft uses a one-way cryptographic hash to create a new anonymized identifier. We then use that identifier, along with the non-identifiable demographic data, to serve ads online. Search query data and web surfing behavior used for ad targeting are associated with this anonymized identifier rather than information that could be used to directly identify a user.

Placing persistent identifiers on an equal footing with data that directly identifies or allows contact with a child, such as the child's full name, e-mail address, and phone number, reduces incentives for businesses to take privacy-enhancing steps to anonymize or de-identify the child's personally identifiable information. Given the choice to use an anonymized or de-identified persistent identifier or, for example, a user's existing e-mail address, some operators may forgo the additional work and expense of using anonymization and de-identification techniques, and instead rely on readily available identifiers that personally and directly identify a child.

In order to minimize the likelihood of such a result, we ask the Commission to consider ways it can continue to encourage the use of anonymization or de-identification techniques – not as a "silver bullet" solution, but as one important way to mitigate privacy risks.

C. It Is Unclear Whether the Commission Has the Necessary Statutory Authority To Expand COPPA's Scope To Include Persistent Identifiers, by Themselves, as "Personal Information."

It is not clear that the Commission has statutory authority to broadly expand the definition of "personal information" to include persistent identifiers that are not otherwise associated with individually identifiable information. The statute defines "personal information" to mean:

[18] *See, e.g.*, Paul Ohm, "Broken Promises of Privacy: Responding To the Surprising Failure of Anonymization," 57 UCLA L. REV. 1701 (2009-2010).

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.[19]

As the Commission acknowledges, its authority to expand COPPA's statutory definition of "personal information" is contained in paragraph (F). In its request for comments, the Commission rejects the notion that persistent identifiers, alone, are out of scope because they permit the contacting of only a specific device, which could be used by many individuals. The Commission notes that other identifiers in the statutory definition could apply to an entire household, such as a home address[20] or a telephone number,[21] and concludes that this demonstrates that Congress did not intend to limit the Commission's authority to include identifiers that single out only one individual. However, this reasoning could be vulnerable to legal challenge as being contrary to the plain meaning of the statutory text ("contacting of a specific individual") and also overlooking the fact that the inclusion of home address and telephone number by Congress as separate paragraphs could just as easily support the opposite conclusion — that they were listed separately in part because they are different in kind than the identifiers contemplated under paragraph (F).

Moreover, the Commission's argument, which focuses on the "specific individual" language, appears to overlook the rest of the statutory text, which requires that the identifier also permit "contacting." An operator that collects a persistent cookie ID from the user's device or computer cannot subsequently use that persistent identifier to "contact" the individual – at least not in the ordinary sense of the word. At most, the persistent identifier enables the entity that sets the cookie to recognize the device if and when the device returns to the website or visits another website within the entity's network.[22]

---

[19] 15 U.S.C. § 6501(8).

[20] *Id.* § 6501(8)(B).

[21] *Id.* § 6501(8)(D).

[22] In this way, a persistent identifier is analogous to the caller ID feature available on many telephones. Caller ID allows the recipient of a call to recognize the caller and to greet the caller by name when answering the call. But it is the caller who "contacted" the recipient of the call, not vice versa. No one would say that the recipient

Because questions can be raised about whether the Commission has the clear statutory authority necessary to expand the definition of "personal information" to more broadly cover persistent identifiers, the revised COPPA Rule may be vulnerable to legal challenge, which inadvertently creates unnecessary costs and uncertainty for consumers, industry, and regulators. Thus, if the Commission decides to proceed with the proposed expanded coverage of persistent identifiers, we strongly urge the Commission to minimize the likelihood of legal challenge by further clarifying the scope of the expansion, as well as the obligations resulting from the expansion, as suggested below.

D. <u>If the Commission Decides To Broaden COPPA's Scope for Persistent Identifiers, It Should More Clarify the Rule and Focus the COPPA Rule Requirements on the Use, Rather Than the Collection, of Persistent Identifiers.</u>

If the Commission decides to broaden COPPA's scope for persistent identifiers, it should, at a minimum, clarify the revised Rule in the following two ways:

- The Rule should make it clear that, in the absence of actual knowledge by the ad network (or similar third-party online service provider) that a particular user is a child, the ad network will not be subject to COPPA if the operator of the website, application, or online service where targeted advertising is displayed represents to the ad network that the website, application, or online service is directed to a general audience, or does not inform the ad network that the website, application, or online service is directed to children under the age of 13. This approach makes it clear that operators of websites and online services have the responsibility for determining whether such a site or service is directed to children and determining whether or not they allow targeted advertising within those sites and services; ad networks and similar third-party online service providers do not have an independent obligation to determine whether a website, application, or online service where advertising is displayed is directed to children under 13 years of age.

- The Rule should also clarify that when an ad network or a similar third-party online service provider recognizes a device (identified by an IP address, cookie ID, or other persistent identifier) visiting a website, application, or online service that it knows to be

---

"contacted" the caller simply because he or she had the ability to check the caller ID. Likewise, a persistent identifier, such as a cookie ID, enables the entity that set the cookie to recognize the device (and, by inference, the individual or individuals who use that device), but the persistent identifier does not permit the entity to "contact" the individual or individuals. Unlike caller ID (which delivers a phone number to the recipient of the call), however, the cookie ID does not provide a mechanism for the entity that set the cookie to later initiate a separate contact with the device that made the original contact. Further, unlike a telephone number or other identifier that does permit the contact of an individual, a persistent cookie ID, were it to be shared with a third party by the entity that set the cookie, would give that third party even less capability of engaging with the individual. Not only would that third party not be able to contact any person using that cookie ID, it would not even allow the third party to recognize the individual should he or she come to the third party's website, since only the entity that set the cookie containing that cookie ID can subsequently read the cookie.

directed to children, that ad network or a similar third-party online service provider is not prevented from collecting information or delivering targeted ads to that same device when it visits other websites, applications, or online services that are directed to a general audience. This approach is consistent with the "actual knowledge" standard for general audience websites and online services and helps ensure that COPPA's requirements are not inadvertently expanded to cover targeted advertising to (or other data collection from) adults who occasionally visit child-directed websites and online services.

Microsoft is encouraged that the Commission recognizes that uses of persistent identifiers for functions that support the internal operations of the website or online service[23] (such as user authentication, improving site navigation, maintaining user preferences, serving contextual advertisements, and protecting against fraud or theft) are necessary and do not raise significant privacy concerns. However, the COPPA Rule could be further improved by clarifying that all of COPPA's requirements are triggered only where persistent identifiers are *used* for broader purposes, and not by the mere *collection* of a persistent identifier.[24]

While we understand that the Commission's revisions are intended to avoid imposing COPPA's requirements on uses of persistent identifiers for functions that support the internal operations of the website or online service, the proposed text is ambiguous because COPPA is a regulatory framework that focuses on data collection. For example, COPPA's notice, parental consent, parental access, data security, and data retention requirements are all triggered by the *collection* of personal information, rather than by its *use*.[25] The discrepancy between the definition of "personal information," which focuses on the use of persistent identifiers, and the

[23] See Section VI below for our additional recommendations for clarifying the definition of "Support for the internal operations of the website or online service."

[24] As revised, the definition of "personal information" includes persistent identifiers where they are "used for functions other than or in addition to support for the internal operations of, or protection of the security or integrity of, the Web site or online service." 76 Fed. Reg. 59804, 59830 (Sept. 27, 2011). We note, however, because the new definition of "support for the internal operations of the Web site or online service" includes activities that are necessary "to protect the security or integrity of the Web site or online service," including this same language in the definition of "personal information" is redundant.

[25] *See, e.g.*, 16 C.F.R. § 312.4(b) (proposing to require the notice on the website or online service to be placed "at each area of the Web site or online service where personal information is collected from children"); *id.* at § 312.5 (stating that an "operator is required to obtain verifiable parental consent before any collection, use, and/or disclosure of personal information from children"); *id.* at § 312.6 (allowing parents to refuse to permit the operator's future collection of personal information and to review any personal information collected from the child); *id.* at § 312.8 (imposing confidentiality, security and integrity obligations on personal information collected from children); *id.* at § 312.10 (adding data retention and deletion requirements that are tied to the collection of personal information from a child online).

substantive COPPA Rule requirements, which focus on data collection, creates ambiguity about how and when an operator would be expected to comply with COPPA's requirements.[26]

If the revisions to the COPPA Rule are primarily intended to restrict the use of persistent identifiers to deliver behaviorally targeted ads to children, then further amendments are necessary to clarify that the COPPA Rule's substantive requirements are triggered only when such information is used, and not when it is collected. For instance, absent parental consent, the Commission could prohibit ad networks and similar third-party online service providers from displaying behaviorally targeted ads to children if they have actual knowledge that the user is a child under the age of 13. Similarly, absent parental consent, operators of websites and online services that are directed to children could be prohibited from allowing behaviorally targeted ads to be used within such websites or online services. However, none of the COPPA Rule's requirements (other than perhaps data security) should be triggered by the mere collection of a persistent identifier.

III. Microsoft Similarly Encourages the Commission To Clarify the COPPA Rule Requirements for Third-Party Geolocation Services.

The proposed COPPA Rule would include a new category of "personal information" that covers "[g]eolocation information sufficient to identify street name and name of a city or town."[27] Microsoft agrees with the Commission that geolocation information raises significant privacy and safety issues, and we support the inclusion of a more explicit geolocation provision in the COPPA Rule's definition of "personal information."

However, third-party geolocation services present many of the same challenges described above for other third-party online services that collect persistent identifiers, such as ad networks. Third-party geolocation services typically are directed to a general audience, but they may be used by operators of websites or applications that are directed to children or that have actual knowledge that a particular user is under 13. Consequently, the same practical difficulties arise if the geolocation service provider is deemed either to have actual knowledge of the user's age or to be directed to children, based solely on the nature or knowledge of the first-party website or online service. At the very least, as with ad networks and other third-party service providers that collect persistent identifiers, a third-party geolocation service should be permitted to rely on a representation made by the first-party operator of the website or application using the geolocation service as to whether the application or service is directed

[26] Unfortunately, the same ambiguity arises in the broader discussions surrounding "do not track" requirements. Persistent identifiers, such as cookie IDs and IP addresses, are automatically and immediately collected at the time a user's browser navigates to the desired website. To the extent any "do not track" requirements govern the collection, and not just the use, of this data, it becomes technically impossible for the Internet to continue functioning in its current form. In contrast, by focusing "do not track" requirements on specific data uses, rather than on data collection, effective notice and choice mechanisms can be provided to consumers.

[27] 76 Fed. Reg. 59804, 59830 (Sept. 27, 2011).

to children. In addition, as described in the next section, such first parties should be permitted to obtain parental consent on behalf of the third-party geolocation service provider.

IV. Parental Notice and Consent Requirements in Cases Where There Are Multiple Operators Should Be Streamlined To Prevent Imposing Undue Burdens on Parents.

Even if the Commission follows Microsoft's request to further clarify ad networks' and other third-party online service providers' responsibilities as proposed in Parts II and III above, the proposed revisions could greatly increase the number of ad networks and other third-party service providers that are subject to the COPPA Rule's requirements.

Requiring operators to provide contact information for and describe the information practices of each ad network and other third-party service provider is unworkable and could confuse parents about who exactly is collecting, using, or disclosing their children's personal information online and who is the appropriate contact for questions. The current rule, which permits the designation of a single operator, provides a much simpler process for parents.[28] Modern websites are frequently a complex amalgam of content and services from many different sources and entities. A single website may use half a dozen different ad networks, plus numerous other third-party services – each of which would have to be specifically identified and described in the privacy notice. This complexity is compounded by the fact that a website may frequently change which ad networks and other third-party service and content providers it uses – sometimes on a daily basis. Consequently, a parent would have a difficult time determining which of these multiple operators to contact with a question or concern. Designating a single operator for this purpose helps avoid this complexity.

In addition, in many cases where ad networks or other third-party online service providers are involved, it would be impractical for the ad networks and other third-party online service providers to each obtain parental consent directly from the parent. As drafted, each of these third parties, who usually are one or more steps removed from the website or service that has the relationship with the child and parent, would need to establish direct relationships with end users of the first-party website or online service, and, to the extent the end user is under the age of 13, would need to establish direct relationships with the child's parent. Even where this might be possible, the process for creating these direct relationships likely would disrupt the user experience and would require more entities to collect more personal information from more consumers than is otherwise the case today.

[28] Additionally, we suggest that the Commission further amend its notice requirements to permit operators to use a web-based contact form in lieu of listing an e-mail address. In our experience, web-based forms are just as effective as e-mail in enabling consumers to contact website operators, but help cut down on the spam and misdirected messages that inevitably result when an e-mail address is published. Web-based forms also help avoid losing legitimate e-mails as a result of spam filtering.

A parent who has provided consent for his or her child to use a particular website or service also might become confused or overwhelmed when he or she receives numerous parental consent requests from third parties who collect personal information from the same website or online service. This frustration could become particularly acute if many of the third-party operators use the credit card method for obtaining parental consent, which would result in a parent having to pay many transaction fees to many different unfamiliar companies just to provide full consent for a single website or online service.

To help alleviate the burdens on parents, Microsoft encourages the Commission to clarify its rules to permit ad networks and other third-party online service providers to rely on the parental consent that is obtained by the first-party operator of the website or online service as long as the first-party operator clearly discloses to the parent that the child's personal information will be disclosed to third-party online service providers. Such disclosure should describe:

- The types of third-party service providers (ad networks, geolocation services, game publishers,[29] etc.) that may receive the child's personal information,
- The types of personal information such third parties may receive, and
- A general description of how those third parties may collect, use, and disclose such information.

The third-party online service providers could then collect, use, and disclose the child's personal information, consistent with the notice provided by the first-party operator and consented to by the parent, without the need to independently obtain consent from the parent. However, if the third-party online service provider seeks to collect, use, or disclose the child's personal information beyond the practices described in the first-party operator's notice, that third party would need to obtain independent parental consent that covers such additional collections, uses, or disclosures.

---

[29] In addition to the ad network and geolocation service examples discussed elsewhere in these comments, the option to rely on notice from the first-party operator is appropriate for gaming services like Xbox LIVE where the parent and child would have direct, authenticated accounts with the service. In such services, both first-party and third-party games run within the service and are essential to provide the online gaming experience that the user requests and, in many cases, has paid for. The Xbox LIVE platform exists so that third-party publishers can plug into it and users can take advantage of cross-platform features and user controls. Console makers need to seamlessly share user and device information with game publishers in order to provide users with innovative online game services – from online gameplay to chat to leaderboards. Subscribers expect this as part of the service. To participate in the online service for the Xbox 360 console, for example, a user must have a valid Xbox LIVE account; consent from a parent, who also must have an Xbox LIVE account, is necessary for under-13 accounts. The parent also can take advantage of parental controls for the console and service to fine-tune sharing, online access and available content. See http://support.xbox.com/en-US/xbox-live/how-to/parental-control, http://support.xbox.com/en-US/xbox-live/how-to/online-safety and http://www.getgamesmart.com/tools/familysettings/. For privacy controls to apply across the platform, Xbox LIVE must share user information so the publisher can know and respect the settings the parent chose for the child.

As the designated operator for COPPA purposes, the first-party operator would field questions from parents about its own privacy practices and would refer the parent to the appropriate third-party online service provider or providers if the question relates to one or more specific third-party online services. This is likely to result in a more satisfactory and effective redress policy because the first-party operator, more so than a parent confronted with a long list of third-party operators, is in a much better position to know which service provider or providers are relevant to the parent's inquiry.

In sum, this approach avoids confusing and overly burdening parents. Parents still receive clear notice that ad networks and other third-party online service providers may collect their children's personal information online. But it will be simpler and easier to navigate when a parent has a question or concern. This approach also aligns with how consumers expect many services, such as online gaming platforms, to work. In addition, this process avoids inundating parents with numerous parental consent requests for a single website or online service and helps ensure that, to the extent the operators rely on the credit card method for obtaining parental consent, a parent is charged only a single minimal fee by a known entity in connection with the parental consent process.

V. Microsoft Agrees That the Definition of "Personal Information" Should Include Photographs, Videos, and Audio, but Encourages the Commission To Clarify That Operators Cannot Gain Actual Knowledge from Such Files.

The current COPPA Rule clearly includes photographs of individuals that are submitted by the child and that are combined with other information such that the combination permits physical or online contacting.[30] Such information raises clear safety concerns, and requiring operators to provide parents notice and to obtain parental consent helps ensure that the child's privacy and safety are protected. Microsoft fully supports expanding this approach to cover video and audio files as well, so that it is explicit that operators who combine video and audio files with other information such that the combination permits physical or online contacting would be subject to COPPA.

The proposed COPPA Rule takes a broader approach, however, adding a new category of "personal information" that covers a "photograph, video, or audio file where such file contains a child's image or voice."[31] Although Microsoft generally supports the principle behind this proposed change, we ask that the Commission provide clear, practical guidance on when a child's posting of photos or other multimedia content would trigger the Rule.

Specifically, Microsoft requests that the Commission clarify that an operator of a general audience site or service will not be deemed to gain actual knowledge from photograph, video, or audio files that contain circumstantial information that suggests a particular user is under 13 years old. For example, if a banner in the background of a photo says "Happy Seventh

[30] 16 C.F.R. § 312.2.

[31] 76 Fed. Reg. 59804, 59830 (Sept. 27, 2011).

Birthday," an operator will not be deemed to have actual knowledge that a pictured child is under 13, even if the operator becomes aware of the photograph. This approach is appropriate because in most cases it will be difficult to know for sure whether the person uploading the file is the same person who is featured in the photograph, video, or audio file. Absent this clarification, many sites – and not just those directed at children – could stop allowing photos and other multimedia content from being uploaded.

VI. Microsoft Agrees That "Support for the Internal Operations of the Web Site or Online Service" Should Be Separately Defined and Expanded, and Asks the Commission To Clarify the Definition and Include Activities That Are Necessary To *Improve* the Website or Online Service and Those Necessary for the Functioning of the Website or Service.

The Commission proposes to separately define the term "support for the internal operations for the Web site or online service" and to expand the current definition to include activities necessary to protect the security or integrity of the website or online service, in addition to activities that are necessary to maintain the technical functioning of the website or online service or to fulfill a child's request.[32] Microsoft supports this approach, but we believe the definition could be further improved with two additional modifications.

First, we suggest adding the phrase "or improve" after the word "maintain." The current definition could be interpreted to permit uses of collected personal information to support internal operations only if the use maintains the status quo, thereby precluding innovation and improvements that will benefit consumers. As long as the data is used to support internal operations of the site or service and is not shared with third parties for other purposes, uses that improve the website or online service do not increase the potential privacy risk to any greater extent than uses that maintain the website or online service, and as such, should be permitted in the same manner.

Second, we suggest removing the word "technical" before the word "functioning." As written, it is unclear how or if the word "technical" limits the kinds of activities that would fall under this definition. If the activity is necessary for the functioning of the website or online service, that should be permitted as necessary for internal operations.

* * *

Microsoft appreciates the opportunity to provide these comments to assist the Commission with its ongoing review of the COPPA Rule. We look forward to continuing to work with the Commission toward our common goals of encouraging the development of innovative online content and services for children while protecting the privacy and safety of children online.

Sincerely,

[32] *Id.* at 59809.

Michael D. Hintze
Associate General Counsel
Microsoft Corporation