Promoting Convenience, Choice, and Commerce on the Net

The NetChoice Coalition
1401 K St NW, Suite 502
Washington, DC 20005
202.420.7482
www.netchoice.org

August 19, 2019
FILED ELECTRONICALLY
Federal Trade Commission

Nomination of Carl Szabo for panelist position for
The Future of the COPPA Rule: An FTC Workshop

NetChoice welcomes this opportunity to nominate Carl Szabo as a panelist for the Federal Trade Commission's (FTC) *The Future of the COPPA Rule: An FTC Workshop*.

Nomination of Carl Szabo as a panelist for the Federal Trade Commission's (FTC) *The Future of the COPPA Rule: An FTC Workshop*

> Carl Szabo is Vice President & General Counsel for NetChoice. As Vice President and General Counsel, Carl analyzes tech-related legislative and regulatory initiatives relevant to online companies. He monitors and analyzes Federal and state legislation including online taxation and privacy issues. Carl is also an adjunct professor of privacy law at the George Mason Antonin Scalia Law School.
>
> Carl works at the NTIA Privacy Multi-Stakeholder process, speaks on panels about burdens to e-commerce, and testifies before state legislatures on proposed legislation. He is well published on COPPA and engaged actively in the recent rule-making on COPPA.
>
> Before joining NetChoice, Carl was an intellectual property attorney at the lawfirm of Wildman, Harrold, Allen & Dixon where he advised clients on privacy, Internet, e-commerce, and contractual matters. He also worked at the lawfirms of Venable and Arnold & Porter.
>
> Carl also worked on copyright, trademark, and anti-piracy both for Motion Picture Association of America (MPAA) and the Entertainment Software Association (ESA).
>
> Before law school, Carl worked at the Federal Trade Commission (FTC) on the staff of Commissioner Orson Swindle, where he helped create and implement the FTC's Consumer Information Security Outreach Plan and assisted the White House in establishing the National Strategy for Cyber Security.
>
> Carl obtained his J.D. and Communications Law Certificate from the Catholic University of America, magna cum laude, and Carl obtained his B.A. in Economics, Managerial Studies, and Policy Studies from Rice University. Carl is licensed to practice law in Washington, DC and is a Certified Information Privacy Professional (CIPP/US)

Regarding necessary updates to COPPA

In addition to nominating Carl Szabo for the workshop, NetChoice submits the following comments on the Children's Online Privacy Protection Act (COPPA) Rule and its implementation by the Federal Trade Commission. As we explain below, NetChoice believes that the present COPPA Rule generally serves the

interests of children, parents, and online services. Our comments reflect concerns about how some of the recent changes to the COPPA Rule would undermine online services children now enjoy. Our comments focus on the following areas:

1. COPPA SHOULD NOT HAVE CREATED SUCH AN OVERLY BROAD DEFINITION OF "PERSONAL INFORMATION" AS THE MODIFIED DEFINITION DOES NOT IDENTIFY AN INDIVIDUAL BUT A DEVICE

2. THE DEFINITION OF "SUPPORT FOR INTERNAL OPERATIONS" SHOULD INCLUDE ACTIVITIES THAT FACILITATE THE TECHNICAL FUNCTIONING OF A WEBSITE

3. CHANGE THE DEFINITION OF PERSISTENT IDENTIFIERS SO THAT PERSISTENT IDENTIFIERS MUST STILL BE COMBINED WITH SOME OTHER PERSONAL INFORMATION TO BE CONSIDERED "PERSONAL INFORMATION"

4. DO NOT INCLUDE SCREEN NAMES, USER NAMES OR IDENTIFIERS USED TO LINK A CHILD'S ACTIVITIES ACROSS SITES IN THE DEFINITION OF PERSONAL INFORMATION, SINCE THIS WOULD REDUCE BENEFITS TO CHILDREN

5. TREATING A FAMILY PHOTOGRAPH OR VIDEO ALONE AS PERSONAL INFORMATION REPRESENTS AN UNAUTHORIZED EXPANSION OF COPPA

6. THE FTC SHOULD NOT REQUIRE PARENTAL CONSENT WHEN THERE IS PASSIVE TRACKING OF CHILDREN BUT NO COLLECTION OF PERSONAL INFORMATION, SINCE SUCH TRACKING PROVIDES BENEFITS TO CHILDREN, AND A PROHIBITION ON TRACKING IS OUTSIDE THE SCOPE OF FTC AUTHORITY UNDER COPPA

7. TREATING "PROMPTING OR ENCOURAGING" AS "COLLECTION" OF PERSONAL INFORMATION IS NOT VIABLE IN TODAY'S SOCIAL NETWORK ONLINE WORLD

8. NEED TO ADDRESS THE COLLECTION OF DATA BY NON-PROFITS

Below, we discuss why recommend revisions to COPPA and discuss how a failure to revise the proposed COPPA Rule changes would impose unintended collateral damage on beneficial online services for children.

1. COPPA should not have created such an overly broad definition of "Personal Information" as the modified definition does not identify an individual but a device

The COPPA rules made persistent identifiers and IP addresses part of the definition of personal information. The FTC's rationale at the time for this expanded definition is to, in part, "'streamline' the

Rule's language."[1] However, the expansion of persistent identifiers to identify a device, not a person, or in the case of COPPA, a child, has likely discouraged development of child directed sites and services.

The FTC should consider abandoning this flawed definition of "persistent identifiers" and return to a more appropriate definition that identifies actual identifiers of individuals.

Persistent identifiers enable necessary online functionality and user services

> New Definition:
> "A persistent identifier, including but 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, where such persistent identifier is used for functions other than or in addition to support for the internal operations of, or protection of the security or integrity of, the website or online service;"[2]

Persistent identifiers enable site functionality that is otherwise not possible. Persistent identifiers allow sites to identify which areas of the site are most and least visited, and where the site should devote its resources to provide the best user experience.

Persistent identifiers identify devices, not people

Persistent identifiers, like cookies, only identify a device—not a person. Consider a family computer. When Microsoft Edge is opened, the actual user might be the child, but it could also be siblings, parents, babysitters, or any visitors to the home. Or consider an iPad. The unique identifier of that device does not indicate if the operator is a child, an adult, or a friend of the family.

So if the collector or user of persistent identifier has no idea who is the user of a device, that identifier cannot be personal information and the FTC should not treat a persistent identifier as such.

2. The definition of "support for internal operations" should include activities that facilitate the technical functioning of a website

As discussed above, we do not agree that all persistent identifiers are personal information. However, if the FTC decides to continue treating persistent identifiers as personal information, the FTC should, at a minimum, amend its definition of "support for the internal operations" exception so it is clear that important site operations are included. Under the new rules, collection of personal information is not subject to COPPA if collected for the "support for the internal operations of the website or online service."[3] The definition is:

> Support for the internal operations of the website or online service means those activities necessary to:
>
> (a) maintain or analyze the functioning of the website or online service;
>
> (b) perform network communications;
>
> (c) authenticate users of, or personalize the content on, the website or online service;
>
> (d) serve contextual advertising on the website or online service or cap the frequency of advertising;

[1] COPPA Rule Review, 16 CFR Part 312, Project No. P104503 at p.18.
[2] COPPA Rule.
[3] COPPA Rule Review, 16 CFR Part 312, Project No. P104503 at p. 25-27.

(e) protect the security or integrity of the user, website, or online service;

(f) ensure legal or regulatory compliance; or

(g) fulfill a request of a child as permitted by §§ 312.5(c)(3) and (4*)*;[4]

Unfortunately, the existing exception is limited to "those activities *necessary* to maintain the technical functioning of the website."[5] The inclusion of "necessary" risks making this exception susceptible to subjective and fluctuating determinations about what is meant by "necessary." Moreover, the use of "necessary" makes the exception too narrow and could prevent many small companies from satisfying COPPA compliance requirements.

Often small companies use third-party service providers to perform valuable—though not technically *necessary*—operations for their websites. For example, site analytics used to identify site traffic is not "necessary" for the technical functioning of a website. However, many sites use third party analytics services to track this information to improve site mechanics and user experiences.

Consider a site that uses persistent identifiers and website analytics to determine which aspects of their site are most visited or which aspects of their site deserve further development. Under the new COPPA rules, a site directed to children might not be able to use such analytics since these services might not be deemed necessary to "maintain the technical functioning" of the website. This means that a site dedicated to helping kids learn math might not use analytics to identify which math lessons children prefer and which problems they struggle to solve. And a site that helps children learn about books might not have the necessary analytics to allocate resources to developing the most popular areas of the site.

The FTC should change its definition of "support for the internal operations" so it is clear that these useful, but arguably not "necessary," site functions to fall within the "support" exception. Below is a recommended edit to this "support" definition:

> *Support for the internal operations of the website or online service* means those activities ~~necessary to maintain~~ that facilitate:

3. Change the definition of persistent identifiers so that persistent identifiers must still be combined with some other personal information to be considered "personal information"

As stated above, NetChoice does not believe that all persistent identifiers are personal information. However, at a minimum, the FTC should only consider a persistent identifier as personal information when the persistent identifier is combined with some other information that would allow contact with a child.

Persistent identifiers identify do not necessarily permit contacting a child

Under prior COPPA rules, persistent identifiers are personal information only when combined with a user's email address.[6] This makes sense since an email address identifies an individual and could therefore enable contacting of a child. Unless it is combined with or contains personal information, a persistent identifier alone does not identify a child, a parent, or any other individual.

---

[4] COPPA Rule at p. 114.

[5] COPPA Rule Review, 16 CFR Part 312, Project No. P104503 at p. 27 (emphasis added).

[6] "Currently, screen names are considered "personal information" under COPPA only when they reveal an individual's email address." *Id.* at p.30.

Under the prior COPPA rule, the FTC recognized that a persistent identifier does not necessarily identify an individual, but instead, identifies a device. That is why the prior COPPA rule required a persistent identifier to be combined with individually identifiable information before the persistent identifier is regarded as personal information.[7] When a browser is used on a family's home computer, the actual user might be the child, but it could also be siblings, parents, babysitters, or any visitors to the home.

While the FTC appears to understand the distinction between identifying a device rather than a child, the new rules abandon this distinction.

This is a clear shift away from protecting children from actual harm to a more theoretical type harm that the FTC typically avoids empowering.

The FTC incorrectly equates persistent identifiers with home addresses and phone numbers

The FTC's decision to consider persistent identifiers and IP addresses as personal information is based on a flawed analogy to home addresses and phone numbers. In the COPPA statute, the definition of personal information includes home address and phone number.[8] It does *not* include persistent identifier or IP address. But the FTC attempts to equate persistent identifiers and IP addresses with home address and phone number by arguing that in both cases an operator is "likely" to be able to contact a specific individual.

The FTC mistakenly compares an IP address to a home address or phone number to justify its inclusion of IP address as personal information.[9] Home addresses and phone numbers rarely change. In contrast, IP addresses regularly change. Household Internet service providers like Comcast and Verizon can and often do change the IP addresses assigned to customer computers. Moreover, for mobile devices, the IP address is constantly changing as a user moves among cell towers.

The FTC's comparison of a persistent identifier to a physical address or phone number is more attenuated than its comparison to an IP address. Persistent identifiers are often anything but persistent. With the clearing of cookies, persistent identifiers are deleted. Persistent identifiers are often and easily changed or removed, which is certainly not true of a home address or phone number.

Since neither IP addresses nor persistent identifiers are comparable to home addresses or phone numbers, the FTC cannot equate them as personal information for COPPA purposes.

Congress affirmatively chose to not list persistent identifiers as personal information in COPPA

The FTC goes beyond the intent of Congress in changing the COPPA to include rule to include IP address and persistent identifiers. The COPPA statute lists home addresses and phone numbers in the definition of "personal information," Congress also intended to include things like persistent identifiers and IP addresses in that definition.[10] In reality, Congress deliberately chose not to include IP addresses and unique identifiers in COPPA.

---

[7] See paragraph (f) to the definition of "personal information." 16 CFR 312.2.
[8] 15 U.S.C. § 6501, *et al*.
[9] COPPA Rule Review, 16 CFR Part 312, Project No. P104503 p.34.
[10] *See, e.g. id.* at p.33-34

IP addresses and persistent identifiers existed well before the enactment of COPPA. Moreover, privacy concerns about persistent identifiers were raised in the 1998 FTC Report to Congress[11] on which much of COPPA's language is based.[12] So when Congress wrote COPPA, it considered and rejected IP addresses and persistent identifiers as forms of personal information. This conclusion is further bolstered by the enumeration of what Congress determined *is* personal information and the fact that persistent identifiers and IP addresses are not included on that list.

Despite the FTC's attempt to expand the definition adopted by Congress, neither persistent identifiers nor IP addresses are like home addresses or phone numbers. Since the FTC failed to properly justify this significant change to the definition of personal information, the FTC should abandon its flawed inclusion of persistent identifiers or IP addresses unless combined with some other form of identifying information collected from a child.

4. Do not include screen names, user names or identifiers used to link a child's activities across sites in the definition of personal information, since this would reduce benefits to children

The new rules added screen and user names to the definition of "personal information," even when they don't include the child's email address or other identifying information, when they are used for functions other than or in addition to support for the internal operations of the website or online service. In addition, the new rule suggests including identifiers that link a child's activities across several sites in the definition of "personal information." Unfortunately, these changes would decrease website services to children and might actually increase the collection of information about children.

> New Definitions:
> (d) A screen or user name where it functions in the same manner as online contact information, as defined in this section;
>
> …
>
> (h) A persistent identifier that can be used to recognize a user over time and across different websites or online services. Such persistent identifier 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;

Under the COPPA statute, for a screen or user name to be treated as personal information it *must* allow the "online contacting of a specific individual."[13] But, contrary to the assertion in the NPRM that these identifiers permit the direct contact of a specific individual online,[14] not all screen or user names enable online contacting or communication. So a broad treatment of screen and user names as personal information may exceed the statutory authority in COPPA.

The FTC does not appear to consider the many benefits of linked identifiers for purposes outside of behavioral advertising. Requiring users to create new screen names or new persistent identifiers may

[11] Federal Trade Commission, *Privacy Online: A Report To Congress*, p.45-46 (June 1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf.
[12] *See* Congressional Record, 105th Congress, Senate p. S8483 (July 17, 1998) (citing the 1998 FTC Report to Congress as the rationale for introducing COPPA).
[13] 15 USC § 6502(8)(c).
[14] COPPA Rule Review, 16 CFR Part 312, Project No. P104503 p.30.

force businesses to collect more information than they might otherwise want or need. Moreover, with each collection, there is an increased chance of data breach or data loss.

For example, if a child has a Scallyroo.com account,[15] this account could be used to login on other sister-sites. This unified login across sites reduces the number of sites storing a child's information and eases the process for obtaining parental consent. However, a prohibition on using an identifier across different websites would diminish the effectiveness of online services designed to enable friends to interact with each other.

Moreover, requiring advance parental consent before use of an identifier across different websites is not adequately justified in the prior NPRM. The FTC states its rationale for this new limitation as "intended to serve as a catch-all category covering the online gathering of information about a child over time for the purposes of either online profiling or delivering behavioral advertising to that child."[16] This rationale appears to only address purported and unproven harms to children and fails to account for the resulting impact of this definitional change on beneficial uses of anonymous identifiers. These problems for sites are further exacerbated due to the limited scope of the "support for internal operations" exception as discussed above.

First, as discussed below, we do not agree that delivering behavioral advertising to children is necessarily harmful. Second, this prohibition extends beyond its intended limitation to "profiling" and "behavioral advertising."

The FTC should not include screen names, user names or identifiers that link a child's activities across different websites in the definition of personal information unless those anonymous identifiers are coupled with identifying information that allows contact with a specific child under 13.

5. Treating a family photograph or video alone as personal information represents an unauthorized expansion of COPPA

> New Definition:
> A photograph, video, or audio file where such file contains a child's image or voice.

Internet evolution now allows parents to quickly share photographs and videos with relatives. When the FTC modified COPPA to include in the definition of "personal information" a family photograph or video without any other identifying information, it reduced the ability of sites to facilitate family photo sharing.

The new rules make a photograph alone--without any other data--personal information. However, the FTC appears to doubt its own change. The justification for this new definition of personal information by stating, "photographs of children, in and of themselves, *may contain* information, *such as embedded geolocation data*, that permits physical or online contact."[17] This statement implies that without the embedded data, no physical or online contact is possible with just a picture.

The COPPA statue limits the FTC's authority only to information that "permits the physical or online contacting of a child,"[18] so the inclusion of photographs and video alone as personal information extends beyond the FTC's statutory authority.

---

[15] A facially COPPA compliant website that seeks parental consent prior to authorizing a user under 13.
[16] COPPA Rule Review, 16 CFR Part 312, Project No. P104503. p. 37-38.
[17] *NPRM* at p. 38-39 (emphasis added).
[18] 15 USC § 6502(8)(c).

Since the existing rules already address the FTC's concerns (pairing a photograph with other information) and since the FTC would exceed its statutory authority, the FTC should alter the NPRM's proposed definition concerning photographs, video, and audio content that include a child to the following:

> Suggested Change to Definition:
> A photograph, video, or audio file where such file contains a child's image or voice <u>that the operator collects online from the child and combines with an identifier that permits the online contacting of that child</u>;

6. The FTC should not require parental consent when there is passive tracking of children but no collection of personal information, since such tracking provides benefits to children, and a prohibition on tracking is outside the scope of FTC authority under COPPA

> Addition to Collects or Collecting:
> (c) passive tracking of a child online.

The FTC should not require parental consent before an operator can "collect" information from a child via "passive tracking" if no personal information is collected.

The passive, anonymous tracking of children through unique identifiers benefits parents and teachers. By using these unique identifiers, parents can more easily tell which sites their child visits and for how long. Teachers can use these identifiers to see if a student did proper online research or to see if students completed their online homework.

Passive, anonymous tracking allows for more appropriate content for children since it helps sites to better monetize their ad-supported content. With this ad revenue, sites directed to children can build more and better content and features. Without the ability to use passive tracking to monetize content, sites would provide less content, erect pay-walls, and/or abandon their child-oriented businesses. To simply dismiss a businesses model without justification is arbitrary and capricious.

Actually, the use of passive tracking to deliver ads to kids is about the same as delivering TV ads to children based on program content, time of day, geographic location, and channel -- a practice the FTC has long allowed.[19] The only meaningful difference between TV ads and passive Internet tracking is that the internet allows the equivalent of tracking which programs were previously watched on a given TV.

Finally, the prohibition of passive tracking is outside the scope of FTC authority in the COPPA statute. The COPPA statute granted the FTC authority to regulate collection of the personal information from a child.[20] The FTC overstepped its authority when making its original rule prohibiting the passive tracking of children, but the FTC can now withdraw this prior overreach.

Because of the benefits of passive tracking, and lacking the necessary statutory authority to prohibit such actions under COPPA, the FTC should allow tracking of children where no personal information is involved.

---

[19] *See* FTC, *Advertising to Kids and the FTC: A Regulatory Retrospective That Advises the Present* (2004), *available at* http://www.ftc.gov/speeches/beales/040802adstokids.pdf.
[20] *See* 15 USC § 6502.

7. Treating "prompting or encouraging" as "collection" of personal information is not viable in today's social network online world

Change to Collects or Collecting:
(a) "Requesting, prompting, or encouraging a child to submit personal information online"[21]

The FTC should not include "prompting, or encouraging" as forms of collection. Such a classification has the unintended consequences of pulling otherwise non-COPPA sites under COPPA regulation.

Social networking has changed the structure of nearly every website. Social media buttons now appear on websites as diverse as WallStreetJournal.com, StateFarm.com, and Epicurious.com.

These buttons allow users to easily connect with their friends' interests, learn more about the site content their friends view, and learn about content their friends like. However, the new rule regards the mere display of these buttons as "prompting or encouraging of a child to submit personal information online"[22] as defined in the "Collection" section of the new rule, since their presence "encourages" the sharing of personal information. If a site "encourages" without prior parental consent, then the site violates COPPA.[23] Since these buttons appear upon loading a webpage, there is no ability to obtain parental consent prior to this "encouragement" of sharing.

For example, a child directed site would be collecting personal information just by having the "Like" button on their site. If the site had not received parental consent before a child landed on their page and loaded the "Like" button, then the site would, under the new rule, violate COPPA.

Finally, prompting or encouraging even affects Teen.com, a "hidden gem" according to Common Sense Media.[24] Teens.com displays social media integration, all before obtaining parental consent.

The likely goal of the COPPA is not to eradicate such social networking features from sites directed to children. However, that is the effect of treating "prompting or encouraging" as collection. NetChoice recommends that the FTC not change COPPA to include "prompting or encouraging" as collection.

8. Need to address the collection of data by non-profits

We recognize that the authority of the FTC is limited to businesses however every day non-profits collect data about children without proper oversight or protections.

As identified in the questions presented, we suggest that the privacy protections afforded not only apply to businesses, but also to all entities, including non-profits.

We have seen how non-profit groups like Common Sense Media (CSM), for example, actively support legislation that has no impact on the data they collect.[25] CSM does not currently comply with General Data Protection Regulation (GDPR)[26] or the not yet implemented California Consumer Privacy Act (CCPA).[27] CSM requires users to surrender name, email address, and zip code before granting access to

[21] COPPA Rule.
[22] COPPA Rule Review, 16 CFR Part 312, Project No. P104503 at p.19-20.
[23] For example, if a cookie is considered PI, when a child visits a site with a "+1" button, the "+1" button is encouraging the child to transmit (or share) that cookie.
[24] Kids-Websites, *available at* http://www.commonsensemedia.org/reviews?media_type=29234&recommended_age=12.
[25] *See, e.g.*, COMMON SENSE MEDIA: "Big Win for Kids and Families: California Passes Landmark Privacy Legislation," https://www.commonsensemedia.org/kids-action/campaign/big-win-for-kids-and-families-california-passes-landmark-privacy-legislation (last visited Nov. 1, 2018).
[26] General Data Protection Regulation (EU) 2016/679.
[27] CA Civ. Code § 1798.100, *et sec.*

research papers.[28] This is just one example that shows the need to expand privacy regulation beyond just businesses.

Likewise, we have seen data breaches at non-profit organizations. Take for example the data breaches at the University of Maryland and Yale University. Since 2005, educational institutions have had an average of over 66 breaches a year.[29] Other non-profits have also had an average of over 9 data breaches since 2005.[30] That is almost one breach per month, yet none of these breaches are subject to most data breach notification laws.

As the FTC's authority is limited to commercial businesses, expended oversight would require allowing the FTC enforcement power over non-profits or allowing enforcement by the Department of Justice who can already take actions against non-commercial entities.

Conclusion

For the reasons expressed above, NetChoice proposes the following edits to COPPA:

> § 312.2 Definitions.
>
> *Collects or collection* means the gathering of any personal information from a child by any means, including but not limited to:
>
> (a) Requesting, ~~prompting, or encouraging~~ a child to submit personal information online;
>
> …
>
> (c) ~~Passive tracking of a child online~~.
>
> *Personal Information* means individually identifiable information about an individual collected online, including:
>
> …
>
> (d) ~~A screen or user name where it functions in the same manner as online contact information, as defined in this section;~~;
>
> …
>
> (g) ~~A persistent identifier that can be used to recognize a user over time and across different websites or online services. Such persistent identifier includes,~~

[28] *See Privacy Policy*, COMMON SENSE MEDIA, https://www.commonsensemedia.org/about-us/our-mission/privacy-policy (last visited Nov. 1, 2018). *See also*, CSMConditioningAccess.png, http://netchoice.org/wp-content/uploads/CSM-conditioning-access.png, showing CSM conditioning access to a report on a visitor's remittance of name, email, and zip code.

[29] *Data Breaches (Organization Type: EDU)*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/data-breaches?title=&org_type%5B0%5D=259 (last visited Nov. 1, 2018). For example, consider the following data breaches from a span of two months in 2018 alone: Trinity College of Nursing and Health Sciences on August 9, 2018; American Institute of Aeronautics and Astronautics on August 7, 2018; Yale University on July 26, 2018; Purdue University on July 13, 2018; and University of Michigan/Michigan Medicine on July 25, 2018. *Id.*

[30] *Data Breaches (Organization Type: NGO)*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/data-breaches?title=&org_type%5B0%5D=263. Examples just from the past three years include: SUIU 32BJ on May 25, 2018; Valley of the Sun YMCA on January 17, 2018; YMCA of San Diego on July 12, 2017; UNM Foundation on May 17, 2017; and Public Health Institute on October 5, 2016. *Id.*

~~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;~~

(h) A photograph, video, or audio file where such file contains a child's image or voice that the operator collects online from the child and combines with an identifier described in this definition;

…

Support for the internal operations of the website or online service means those activities ~~necessary to~~

…

Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include:

(i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan;

(ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

(iii) Having a parent call a toll-free telephone number staffed by trained personnel;

(iv) Having a parent connect to trained personnel via video-conference;

(v) Verifying a parent's identity by checking a form of government- issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete; ~~or~~

(vi) Provided that, an operator that does not "disclose" (as defined by §312.2) children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email or

(vii) using a digital certificate that uses public key technology, using e-mail, or similar electronic method, coupled with additional steps to provide assurances that the person providing the consent is the parent,

…

Please note that the above edits do not represent an exhaustive list of our recommended edits, and we welcome the opportunity to further work with the FTC on the language of the COPPA.

We thank you for your consideration and we ask that you recognize the impact even the smallest changes to COPPA will have on websites that beneficially serve our nation's children.

Sincerely,

Carl M. Szabo
Vice President and General Counsel
NetChoice