



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

December 22, 2011
FILED ELECTRONICALLY
Federal Trade Commission
In the Matter of COPPA Rule Review, P104-503

Comments of NetChoice on the Children’s Online Privacy Protection Rule Review

NetChoice welcomes this opportunity to comment 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 proposed changes to the COPPA Rule would undermine online services children now enjoy.

NetChoice is an association of online services and e-commerce companies, working to promote the integrity and availability of the global Internet. NetChoice is significantly engaged in privacy and safety issues in state capitals, Washington DC, and international Internet governance organizations.

We focus our response to the request for comments in nine specific areas:

- 1. The FTC should not consider all persistent identifiers as “personal information”**
- 2. The definition of “support for internal operations” should include activities that facilitate the technical functioning of a website**
- 3. Change the proposed definition 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. Do not treat a family photograph or video alone as “personal information” as this is 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. The FTC should not remove the sliding scale, including email plus, as a means of parental consent**
- 9. The FTC should not remove the single point of contact option for site operators**

Below, we discuss why some of the changes proposed in the NPRM should be rejected, recommend revisions to some of the FTC’s other proposals, and discuss how a failure to revise the proposed COPPA Rule changes would impose unintended collateral damage on beneficial online services for children.

1. Persistent identifiers are not “personal information” as they do not identify an individual but a device

The NPRM proposes to include a persistent identifier in the definition of personal information. The FTC’s rationale for this expanded definition is to, in part, “‘streamline’ the Rule’s language.”¹ However, the FTC should not consider persistent identifiers as personal information as they only identify a device, not a person, or in the case of COPPA, a child.

Persistent identifiers enable necessary online functionality and user services

NPRM Proposed 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.

Now consider a children’s website like OurWorld.com. OurWorld.com uses a persistent identifier to eliminate the need for children to login each time they visit the site. Moreover, the persistent identifier enables some of the general functionality of the site.

Persistent identifiers identify devices, not people

Persistent identifiers, like cookies, only identify a device—not a person. Consider a family computer. When Internet Explorer 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 treat 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 NPRM, collection of personal information is not subject to COPPA if

¹ COPPA Rule Review, 16 CFR Part 312, Project No. P104503 at p.18.

² *Id.*

³ *Id.* at p. 25-27.

⁴ *Id.* at p. 114.

⁵ *Id.* at p. 27 (emphasis added).

⁶ “Currently, screen names are considered “personal information” under COPPA only when they reveal an individual’s name or other identifying information.” COPPA Rule Review, 16 CFR Part 312, Project No. P-104503

⁷ See paragraph (f) to the definition of “personal information.” 16 CFR 312.2.

collected for the “support for the internal operations of the website or online service.”³ The proposed definition is:

Support for the internal operations of the website or online service means those activities necessary to maintain the technical functioning of the website or online service, to protect the security or integrity of the website or online service, or to fulfill a request of a child as permitted by §§ 312.5(c)(3) and (4), and the information collected for such purposes is not used or disclosed for any other purpose.⁴

Unfortunately, the proposed 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 services like Google Analytics to track this information to improve site mechanics and user experiences.

Consider a site like Fanlala.com 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 COPPA NPRM, a site directed to children, like Fanlala.com, 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 the technical functioning of the website or online service, to protect the security or integrity of the website or online service, or to fulfill a request of a child as permitted by §§ 312.5(c)(3) and (4), and the information collected for such purposes is not used or disclosed for any other purpose

3. Change the proposed definition 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.

³ *Id.* at p. 25-27.

⁴ *Id.* at p. 114.

⁵ *Id.* at p. 27 (emphasis added).

Persistent identifiers identify do not necessarily permit contacting a child

Under the existing COPPA rule, 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.

Under the existing COPPA rule, the FTC recognizes that a persistent identifier does not necessarily identify an individual, but instead, identifies a device. That is why the existing COPPA rule requires 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 proposed NRPM definition abandons this distinction.

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.

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

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.

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

The FTC wrongly suggests that because 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.

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 Congress¹¹ 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 fails to properly justify this significant change to the definition of personal information, it should not include 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 NPRM proposes adding 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 NPRM 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.

NPRM Proposed Definitions:

(d) A screen or user name where such screen or user name is used for functions other than or in addition to support for the internal operations of the website or online service.

(h) An identifier that links the activities of a child across different websites or online services and a screen or user name where such screen or user name is used for functions other than or in addition to support for the internal operations of the website or online service;¹³

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.”¹⁴ But, contrary to the assertion in the NPRM that these

¹⁰ See, e.g. *id.* at p.33-34

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 *Id.* at p.113.

¹⁴ 15 USC § 6502(8)(c).

identifiers permit the direct contact of a specific individual online,¹⁵ 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 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,¹⁶ this account could be used to login on other sister-sites (much like the Google login is used for both Gmail and Google Reader). 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 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."¹⁷ 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

NPRM Proposed Definition:

A photograph, video, or audio file where such file contains a child's image or voice.¹⁸

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

The NPRM would make a photograph alone--without any other data--personal information. However, the FTC appears to doubt its own recommended change. The NPRM justifies this new definition of personal information by stating, "photographs of children, in and of themselves, *may contain*

¹⁵ COPPA Rule Review, 16 CFR Part 312, Project No. P104503 p.30.

¹⁶ A facially COPPA compliant website that seeks parental consent prior to authorizing a user under 13.

¹⁷ COPPA Rule Review, 16 CFR Part 312, Project No. P104503. p. 37-38.

¹⁸ *Id.* at p. 114.

information, *such as embedded geolocation data*, that permits physical or online contact.”¹⁹ This statement implies that without the embedded data, no physical or online contact is possible with just a picture.

The COPPA statute limits the FTC’s authority only to information that “permits the physical or online contacting of a child,”²⁰ so the inclusion of photographs and video alone as personal information extends beyond the FTC’s statutory authority.

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 NPRM Definition:

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 that permits the online contacting of that child;

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

NPRM Proposed Addition To Collection:

The passive tracking of a child online.²¹

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.²² 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

¹⁹ *Id.* at p. 38-39 (emphasis added).

²⁰ 15 USC § 6502(8)(c).

²¹ COPPA Rule Review, 16 CFR Part 312, Project No. P104503 p.22.

²² 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>.

child.²³ 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.

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

NPRM Proposed Change to “Collection”:

“Requesting, prompting, or encouraging a child to submit personal information online”²⁴

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. “Like,” “Tweet This,” and “+1” buttons now appear on websites as diverse as WallStreetJournal.com, StateFarm.com, and Epicurious.com. These buttons also exist on sites directed to children, like MyModel.com and GirlSense.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 NPRM would regard the mere display of these buttons as “prompting or encouraging of a child to submit personal information online”²⁵ as defined in the “Collection” section of the NPRM, since their presence “encourages” the sharing of personal information. If a site “encourages” without prior parental consent, then the site violates COPPA.²⁶ Since these buttons appear upon loading a webpage, there is no ability to obtain parental consent prior to this “encouragement” of sharing.

For example, MyModel.com would be collecting personal information just by having the “Like” button on their site. If MyModel.com had not received parental consent before a child landed on their page and loaded the “Like” button, then MyModel.com would, under the NPRM, violate COPPA. Likewise GirlSense.com would face the same COPPA liability for making a “Tweet” button available.

Finally, prompting or encouraging even affects Teen.com, a “hidden gem” according to Common Sense Media.²⁷ Teens.com displays Facebook, Twitter, and Tumblr integration, all before obtaining parental consent.

The likely goal of the NPRM 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.

²³ See 15 USC § 6502.

²⁴ COPPA Rule Review, 16 CFR Part 312, Project No. P104503 p.22.

²⁵ *Id.* at p.19-20.

²⁶ 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.

²⁷ Kids-Websites, *available at*

http://www.common sense media.org/reviews?media_type=29234&recommended_age=12.

8. The FTC should not remove the sliding scale, including email plus, as a means of parental consent

NPRM Proposed Forms of Consent:

Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include: providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or an electronic scan; permitting a parent to use a credit card in connection with a monetary transaction; having a parent call a toll-free telephone number staffed by trained personnel; having a parent connect to trained personnel via video-conference; or, verifying a parent's identity by checking a form of government-issued identification against databases of such information, provided that the parent's identification is deleted by the operator from its records promptly after such verification is complete.²⁸

Removal of the sliding scale as a form of parental consent will prevent some parents from giving parental consent, impose financial hardships on companies, and expose parents to increased privacy risks.

The FTC should make it easier for parents to grant consent, not make it harder

The FTC recognized the overwhelming success of the sliding scale approach, such as email plus.²⁹ But the FTC wants to ignore this success because it has presumably inhibited the development of other methods of consent.³⁰

If the FTC removes email plus as a means of parental consent under COPPA, the remaining options for parental verification would be more difficult for lower-income or immigrant families. Removing email plus would require parents to grant consent via mail, fax, telephone, or credit card.³¹ This means that a family must have access to one of these technologies to provide consent. But over 55 percent of US households making less than twenty-five thousand dollars don't have credit cards³² and few have fax machines. Moreover, some families don't have government issued IDs (for example, over "25 percent of voting-age African Americans nationwide have no current government-issued photo ID"³³). So eliminating email plus and making verifiable parental consent more dependent on other methods of verification hurts these families most.

Instead of eliminating email plus, the FTC should embrace the success of this program and find ways to make obtaining parental consent easier.

²⁸ COPPA Rule Review, 16 CFR Part 312, Project No. P104503 pp. 68-69.

²⁹ "Email plus has enjoyed wide appeal among operators, who credit its simplicity. Numerous commenters, including associations who represent operators, support the continued retention of this method as a low-cost means to obtain parents' consent." COPPA Rule Review, 16 CFR Part 312, Project No. P104503 p. 67

³⁰ *Id.*

³¹ 16 C.F.R. § 312.5.

³² US Census, *Usage of General Purpose Credit Cards by Families: 1995 to 2007*, available at <http://www.census.gov/compendia/statab/2012/tables/12s1189.pdf>.

³³ Brennan Center, *Citizens Without Proof: A Survey Of Americans' Possession of Documentary Proof of Citizenship and Photo Identification*, available at http://www.brennancenter.org/page/-/d/download_file_39242.pdf.

If email plus is de-authorized, some child-oriented sites may stop serving children

Email plus is how dozens of child-oriented websites comply with COPPA today. This method provides a reliable, inexpensive way for small sites directed to children to operate. However, if the FTC flips the switch to de-authorize email plus as a form of parental verification, many of these sites will likely stop serving children rather than incur the high costs of phone or video verification, or the high legal liability associated with COPPA. So if the FTC flips the switch on email plus, they may also be turning off the lights on many small websites.

Along with privacy concerns is the difficulty and cost of obtaining parental consent without email plus or the sliding scale. The FTC stated in the NPRM that it foresees these high costs of compliance, which fall especially hard on small businesses, stating:

In order to comply with the rule's requirements, *website operators will require the professional skills of legal ... and technical ... personnel ...* and that approximately 80% of such operators would qualify as small entities under the SBA's Small Business Size standards.³⁴

The FTC should avoid imposing these additional costs and also creating a barrier to new entrants due to increased costs of COPPA compliance.

Privacy pitfalls with other methods of parental consent

Removal of the email plus mechanism would force online services for children to collect additional personal information to verify parental consent. It would thereby increase privacy pitfalls, discouraging parents from granting consent due to the more sensitive nature of information requested. It would also increase costs on sites and services directed to children, discouraging incumbent and new entrants from offering these services to children.

To verify parental consent, under the NPRM, online services would require parents to provide personally identifying data (such as credit card information). As a result, private companies would have to store vast amounts of parents' personal information and, by doing so, increase customers' vulnerability to security breaches and identity theft.

For example, a company presently using email plus only needs a parent's name and email address to obtain consent. However, without such a method, these same services would need information such as driver licenses, credit card numbers, or even bank information to verify parental consent. Not only does this further complicate the process for obtaining parental consent, but it would also increase privacy risks.

A 2008 report by the Berkman Center's Internet Safety Technical Task Force did not recommend remote age and identity verification for use by online forums and social networks, saying, "*there are significant potential privacy concerns and security issues given the type and amount of data aggregated and collected by the technology solutions...*"³⁵

To better allow parents to provide COPPA consent while avoiding additional privacy pitfalls, the FTC should not remove the sliding scale method of parental consent.

³⁵ John Palfrey et al., *Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States* (2008), available at <http://cyber.law.harvard.edu/pubrelease/isttf/>

9. The FTC should not remove the single point of contact option for operators as it will add confusion and prove operationally difficult

The FTC proposes to “aid” parents who have inquiries about a website by requiring the COPPA notice to parents to include the contact information for all “operators” of a website or online service rather than maintaining the current rule which permits designation of a single operator as the parents’ contact point. While NetChoice typically favors increased transparency to users and parents, this change will not aid parents as the FTC intends. Instead, it will create more effort and confusion for parents.

Under the existing COPPA rule, the privacy notice to parents must include the contact information of all operators collecting personal information from children. However, one operator can be designated as the point-of-contact responsible for responding to all inquiries from parents concerning the operators’ privacy policies and use of children’s information. This eliminates the need for a parent to cull through multiple entities that meet the definition of an “operator” to try to determine where their inquiry should be sent, or, alternatively, to send their inquiry to all the operators listed even if they may not have the information requested. The current one point-of-contact approach makes it much easier for parents to obtain relevant information about the site’s practices than would be the case if all operators were listed as points-of-contact.

Moreover, the current COPPA rule does not require operators to waste resources unnecessarily replicating contact departments. The proposed change will present operational challenges as well, in terms of coordinating among multiple contacts, and ensuring that multiple names and contact information remain current. This will be especially true if the Commission adopts its proposal to include persistent identifiers in the definition of “personal information,” or fails to expand and clarify the “support” definition as suggested in these comments, as that may increase the number of entities that are deemed “operators” that “collect” personal information from children.

Finally, there is no evidence that parents have had problems with the existing single contact approach or that the current approach has failed to provide parents with the information they need. In fact, the single point-of-contact has been a win/win for parents and operators and should not be abandoned.

10. Conclusion

For the reasons expressed above, NetChoice proposes the following edits to the NPRM’s proposed COPPA changes:

§ 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 such screen or user name is used for functions other than or in addition to support for the internal operations of the website or online service;~~

...

(g) ~~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;~~

(h) ~~An identifier that links the activities of a child across different websites or online services;~~

(i) 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 maintain~~ that facilitate the technical functioning of the website or online service, to protect the security or integrity of the website or online service, or to fulfill a request of a child as permitted by §§ 312.5(c)(3) and (4), and the information collected for such purposes is not used or disclosed for any other purpose

...

Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include: providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or an electronic scan; permitting a parent to use a credit card in connection with a monetary transaction; having a parent call a toll-free telephone number staffed by trained personnel; having a parent connect to trained personnel via video-conference; 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, or, verifying a parent's identity by checking a form of government-issued identification against databases of such information, ...

...

§ 312.4 Notice

...

(1) Each operator's contact information, which at a minimum, must include the operator's name, physical address, telephone number, and email address; Provided that: the operators of a website or online service may list the name, address, phone number, and e-mail address of one operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or

maintaining personal information from children through the website or online service are also listed in the notice

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 NPRM.

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,


Steve DelBianco
Executive Director, NetChoice


Carl M. Szabo
Policy Counsel, NetChoice

NetChoice is an association of online services and e-commerce companies, with the shared goal of promoting convenience, choice and commerce on the Net. More information about NetChoice can be found at www.netchoice.org