

**Before the
Federal Trade Commission**

**In the Matter of the Request for Comments
Regarding Children’s Online Privacy
Protection Rule Review**

Matter No. P104503

COMMENTS

OF

THE INTERNET COMMERCE COALITION.

Jim Halpert, General Counsel
Kate Lucente, Counsel
500 8th Street, NW
Washington, DC 20004

December 23, 2011

December 23, 2011

FILED ELECTRONICALLY

Federal Trade Commission

**In the Matter of the Request for
Comments Regarding Children's Online Privacy Protection Rule Review
Matter No. P104503**

Comments of the Internet Commerce Coalition

The Internet Commerce Coalition ("ICC") appreciates the opportunity to comment on proposed revisions to the Children's Online Privacy Protection Rule ("COPPA Rule"). The ICC's members include leading Internet and e-commerce companies and trade associations: Amazon.com, AOL, AT&T, CareerBuilder, Comcast, eBay, Google, Monster.com, Time Warner Cable, Verizon, TechAmerica and US Telecom. The ICC's general counsel helped to draft the COPPA statute in 1998.

The ICC strongly supports the Commission's goal of guarding the privacy of children who use the Internet and with updating the COPPA Rule to address challenges posed to the protection of children's privacy online. At the same time, we believe that some of the proposed revisions to the COPPA Rule are unduly burdensome and may actually undermine the protection of children online. The Commission should be careful to calibrate the proposed Rule so that it does a better job of creating safer online environments for children, without imposing unnecessary burdens on operators.

We are concerned that expanding the scope of the COPPA Rule, to apply the full panoply of COPPA protections to the collection or use of IP addresses, device identifiers, or location information, absent any other identifying information, would create significant barriers to commercial children's sites that have strong privacy practices and are careful not to collect personal information. It would also force these sites to collect additional personal information to satisfy COPPA's parental verification requirements. We are likewise concerned that the proposed Rule's new definition of personal information would harm the quality and amount of free educational content and child-friendly fora currently available on the Internet. These overly broad definitions of personal information also risk being unworkable if the Commission were to apply them in a similarly categorical way in its forthcoming privacy framework.

I. Application of COPPA Rule to IP Addresses and Other Persistent Identifiers

Both as a matter of law and as a matter of policy, we do not believe that an IP address or a device identifier itself, when not in combination with personal information, should be treated as personal information under the stringent COPPA Rule.

As a matter of law, IP addresses alone are not personal information under the COPPA definition. Unlike a phone number, email address or a home address, one cannot use an IP address to contact an individual. The only way that IP addresses could become personal information is under 15 U.S.C. § 6501(8)(F), which allows the Commission to include as personal information “any other identifier that the Commission determines permits the physical or online contacting of a specific individual.” However, it is not possible to contact an individual via an IP address alone, and certainly not a specific individual. Anyone who would want to contact a specific individual using just an IP address cannot do so with any degree of reliability because they do not know whether the same specific individual is connected to the network through the IP address or device, whether the device itself is still connected to the Internet, or whether the IP address or device is shared; nor would they know whether the individual using the device is a child under the age of 13.

The COPPA Rule’s definition of personal information must be limited to data that reasonably identifies an individual, such that it “permits the physical or online contacting of a specific individual.” 15 U.S.C. § 6501(8)(A)(F). Cookies, IP addresses, and device IDs do not provide a link to a specific individual unless they are linked to personal information.

Designating IP addresses, device identifiers, or location information as personal information would not be sound public policy in the context of the COPPA Rule’s rigorous requirements. It would be a major departure in U.S. Internet law and could significantly hinder the way that child-oriented websites operate. As the Commission’s Notice of Proposed Rulemaking (“NPRM”) acknowledges, IP addresses are an integral part of how the Internet operates and how website operators make available and improve content for site visitors.

Mechanically applying the privacy staff report position that IP addresses and device identifiers are personal information is not workable in the context of COPPA. An IP address, in itself, is not personal information. It may become personal information when it is combined with other data sources, such as when it is associated with other personal information about an individual user and is used to track that user’s movements across websites. Furthermore, applying the many fair information practices embodied in the COPPA Rule to IP addresses, device identifiers or location information when not combined with personal information would be overbroad and unduly restrictive.

The real concern driving this aspect of the NPRM seems to be tracking and profiling known minors across many websites. There is a distinct difference between the collection and use of an IP address to provide website content or contextual advertising on a site to a user and to analyze site usage and content, as opposed to maintaining and using IP address in conjunction with other identifying information across multiple sites to profile a particular child. Accordingly, the Commission should take a more targeted approach that focuses on the tracking of a known child online, across sites, not the online collection of these identifiers or other uses of non-personal information.

We appreciate that the proposed COPPA Rule attempts to recognize the important role IP addresses play in websites’ operations by carving out the use of IP addresses solely to support the internal operations of a website. However, the definition of “support for the internal operations” of a website is too narrow – under the proposed rule it is limited to only those uses “necessary to

maintain the technical functioning of the Web site or online service, to protect the security or integrity of the Web site or online service, or to fulfill a request of a child as permitted.” This list of ‘exempt’ collections is incomplete and risks quickly becoming outmoded. In addition, the proposed addition to the definition of personal information of “an identifier that links the activities of a child across different Web sites or online services” adds a catch-all that makes the collection of persistent identifiers by 3rd parties impossible, even for contextual advertising or by an ad network that uses IP addresses across sites for necessary functions like fraud detection.

The expansion of the definition of personal information to include “persistent identifiers” such as IP addresses, cookies and device identifiers would be counter-productive. It would force the collection of even more data by operators newly subject to COPPA, which would undermine children’s privacy, as these operators would be obligated to collect large amounts of information in order to seek verifiable parental consent. Such an expanded framework would require a website operator to seek additional data from children (and parents) to enable the sites to obtain verifiable parental consent for data collection that would otherwise reasonably be considered non-personally identifying.

For example, if a network advertiser were to offer any advertising services (even contextual) on sites directed at children, it would have to collect the personal information of a child and adult to enable verifiable parental consent, rather than providing services that rely on non-individual identifiers such as cookies. In this context, the underlying website operator would also have to collect and pass information necessary for verifiable parental consent to the ad provider, which would raise additional security and privacy risks.

Further, much web content is free because web operators are able to, without identifying individuals, place advertising and collect traffic data to enable these advertisers to measure website traffic and advertisement footprint. Including IP addresses, cookies and device identifiers in the definition would seriously jeopardize operators’ abilities to offer free content. Also, as more Do Not Track solutions come online, reliance on rigid verifiable parent consent is a less and less narrowly tailored solution that would significantly restrict the availability of advertising to support commercial child-oriented sites with valuable content for children.

In the broader context of Internet privacy, the implications of defining personal information under COPPA so expansively as to cover even the internal use of IP addresses, device identifiers, and location information would set an unworkable precedent for other privacy frameworks. It is neither necessary nor practicable to apply COPPA or other fair information practices to all data in all contexts – rather, data protection measures must be calibrated for different types and uses of data and for different settings.

II. The Statutory Definition of Personal Information Does Not Permit Some of the Proposed New Data Elements

The ICC fully agrees with the Commission that mobile apps, “Internet-enabled gaming platforms, voice-over-Internet protocol services, and Internet-enabled location based services” are online services covered by COPPA, if directed at children under the age of 13 (NPRM at 16). We also consider geo-location information gathered from such online services, which identifies

the street number and the “street name and name of a city or town,” to fit within the statutory definition of personal information, as this information together permits contacting a child.

However, some of the identifiers in the Commission’s proposed Rule exceed the statutory scope of COPPA’s definition of personal information (15 U.S.C. § 6501(8)(A)), because they would not permit the locating or contacting of a child. For example, a “photograph, video, or audio file where such file contains a child’s image or voice” would **not** permit the locating or contacting of a particular child, unless the file also contained additional personal information such as the child’s first and last name; neither would a screen name nor other user name if a child cannot be contacted using that name. Also, as explained above, IP address and other persistent identifiers link an operator to a particular device, not a particular child.

In addition, location information that is not linked to some additional identifying information does not permit contacting a particular child.. The Commission’s proposal to define geo-location information as data “sufficient to identify a street name and name of city or town,” in the absence of any additional identifier, exceeds the scope of personal information intended to be covered by COPPA. The Commission points out that any geo-location information providing precise enough location information “to identify the name of a street and city or town” is already covered by § 312.2. However, the language of § 312.2 provides that “personal information” includes “*a home or other physical address* including street name and name of a city or town.” The proposed Rule refers only to street name and city or town. In contrast to the statute and the COPPA rule, it does not specifically require that the information identify a home or other physical address, and it ignores a critical part of a home or physical address – the street number. It is the street number, plus the street name, and the name of the city or town that provides sufficient information to identify a home or other physical address – without a street number the post office is unable to deliver mail to someone’s address. The street number is an integral part of an address, and without it, a person can not be contacted at their “home or physical address.”

III. Verifiable Parental Consent

We are also concerned that the proposed elimination of the “email plus” parental verification method would further chill the development of safe online sites for children, rather than encourage the development of other verification mechanisms. COPPA has been very effective at curbing abusive marketing practices to children, but far less effective at leaving room for online communications fora for children. In particular, in combination with adding IP addresses and persistent identifiers to the definition of personal information, tightening parental consent for use of a service could significantly complicate the operation of child-friendly fora and further discourage operators from offering such.

There is no indication that eliminating “email plus” verification under all contexts will encourage the development of “more reliable” methods of parental consent, even though the Commission also proposes to allow parties to submit for approval additional parental consent mechanisms – a process that could prove to be cumbersome and time consuming. Rather, if anything, it seems likely that eliminating email plus will lead to the collection of more sensitive types of personal information from parents – such as credit card numbers and government identification numbers – information that, despite security precautions, imposes a greater risk of financial and identify fraud.

We thank you for considering our views.

Sincerely,

Jim Halpert, General Counsel
(202) 799-4441

Kate Lucente, Counsel
(813) 222-5927