Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580

In the Matter of	)	
	)	
Implementation of the	)	Docket No. 339
Children's Online Privacy Protection Rule	)	Project No. P104503

INDIVIDUAL COMMENTS OF THE

CENTER FOR DEMOCRACY & TECHNOLOGY

John B. Morris, Jr
Emma J. Llansó
Mangesh Kulkarni
Center for Democracy & Technology
1634 I Street, NW, Suite 1100
Washington, DC 20006
(202) 637-9800

Dated: June 30, 2010

TABLE OF CONTENTS

Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580

In the Matter of	)	
	)	
Implementation of the	)	Docket No. 339
Children's Online Privacy Protection Rule	)	Project No. P104503

INDIVIDUAL COMMENTS OF THE
CENTER FOR DEMOCRACY & TECHNOLOGY

The Center for Democracy & Technology ("CDT") respectfully submits these comments in response to the Request for Public Comment ("RFC") on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule ("COPPA Rule" or "the Rule").[1] CDT has also today joined with the Progress and Freedom Foundation and the Electronic Frontier Foundation in a broader set of Joint Comments, separately submitted.[2] This document provides more detailed responses to many, but not all, of the questions in the RFC. We appreciate the opportunity to express our views on the vital questions raised in this proceeding. CDT's comments on specific questions raised in the RFC are set out below in the order in which they arise in the RFC.

I. Question 1: Is there a continuing need for the Rule?

The COPPA Rule governing the collection of data from minors age twelve and under is one component of a comprehensive strategy for online child safety. The rule continues to be useful in helping to protect younger minors from predatory marketing schemes and other inappropriate uses of children's personal information.[3] Beyond COPPA, parents have access to a wide range of parental control tools and technologies to assist them in guiding their children online and helping them to take advantage of the numerous educational and entertainment opportunities available on the Internet. The goal of COPPA has been to limit the collection of personal information from children and to encourage and enhance parental involvement in children's online activities. These goals continue to be relevant today and the need for a rule that promotes these goals persists.

---

[1] 16 C.F.R. § 312.

[2] *See* Joint Comments of Center for Democracy & Technology, Progress and Freedom Foundation, and Electronic Frontier Foundation (submitted June 30, 2010) ("Joint Comments").

[3] "The Act and the Rule have been effective in helping to protect the privacy and safety of young children online." FTC, IMPLEMENTING THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT: A REPORT TO CONGRESS at 1*,* Feb. 2007, www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf [hereinafter *2007 COPPA Implementation Report*].

II. Question 1a: Have changes in technology, industry, or economic conditions affected the need for or effectiveness of the rule?

New technologies such as interactive gaming and television, social networking, and mobile applications have created many new ways for children to connect online. The COPPA statute and Rule are both written broadly enough to encompass these new technologies without the need for new statutory language. The definition of "Internet" in both the statute and the Rule is device-neutral, covering "the myriad of computer and telecommunications facilities, including equipment and operating software, which comprises the interconnected worldwide network of networks" that transmit data using TCP/IP or related protocols.[4] Similarly, the term "online service" can reach social networking and many other new communications methods. Thus the Rule remains effective in addressing children's use of the Internet as the available technology and platforms that they employ continue to evolve.

The availability of sophisticated parental control tools has also increased dramatically since the Rule was first issued, giving parents a greater ability to set their own standards for what information their children can access and share online. While the Rule sets an appropriate baseline in preventing sites directed at minors twelve and under from collecting personal information from children without their parents' consent, concerns about online child safety that go beyond this particular issue can be and are properly addressed by user and parental empowerment technologies. The Commission provides a number of educational resources that give parents information about the availability of tools such as filtering and blocking software, applications that enforce time limits on a child's Internet or computer use, web browsers designed for children, child-oriented search engines, and monitoring tools that allow parents to review what their children see when they surf the Internet.[5]

III. Question 1b: What are the aggregate costs and benefits of the Rule?

As we discuss in the Joint Comments, the Rule has led to increased costs for operators of child-oriented sites and services, and higher barriers to entry for innovators in this space. Operators of sites who must comply with COPPA's verifiable parental consent requirement may have to employ chat-room supervisors, handle parental inquiries, and process COPPA permission forms at significant expense.[6] Verifiable parental consent procedures are costly to implement and very few website operators can afford to undertake COPPA compliance.[7] Complying with COPPA presents a barrier to entry that is often insurmountable for small start-ups and others who might otherwise seek to create new online resources for kids. Innovation in creative and educational websites for children twelve and under has thus been suppressed, particularly when compared to

---

[4] 16 C.F.R 312.2

[5] Net Cetera: Parental Controls, http://www.onguardonline.gov/topics/net-cetera-parental-controls.aspx (last visited June 27, 2010).

[6] Ben Charny, *The Cost of COPPA: Kids' Site Stops Talking*, ZDNet (September 13, 2000), http://www.zdnet.com/news/the-cost-of-coppa-kids-site-stops-talking/110410

[7] *See Id.* (employing chat-room supervisors, monitor phone lines to answer parents' questions and process COPPA cost website $200,000 per year); Privacilla.org, Children's Online Privacy Protection Act, http://www.privacilla.org/business/online/coppa.html (last visited June 27, 2010) (COPPA raised the cost of serving children by $50,000 to $100,000 per year).

the profusion of sites and services developed for an audience of older minors and adults. Further, children are often prohibited from using such sites, depriving children of the benefits of innovation that occurs in the adult space.[8] In addition, innovation in developing procedures to obtain parental consent has been limited as websites choose to use the methods suggested by the FTC out of fear that a more innovative method could lead to liability.[9]

IV. Question 2: What have been the benefits and costs of the Rule for children, parents, or other consumers?

The Rule has been successful in limiting the collection of personal information from children.[10] As we discuss in our Joint Comments, the Rule has also been effective in increasing parental involvement in children's online activities and has led to websites collecting less information from children.[11]

As discussed in Section III above, the Rule has had a chilling effect on innovation in the child-oriented online space. Verifiable parental consent procedures are costly to implement, which leads most websites to prohibit minors under 13 from using their sites. The cost of verifiable parental consent procedures also prevents many small start-up firms from offering innovative sites and services to younger minors. The fact that a website is "COPPA compliant", and that parents have been in direct contact with the site in order to give their consent to the collection of information from and about their child, can also give parents a false sense of security regarding the safety of their children on that site and the types of interactions they may engage in. COPPA was enacted in order to restrict the collection of personal information from children; its regulations were not designed to dispel the need for parental supervision of children's online activity.

V. Question 3b: What have been the costs of the Rule to operators?

Operators of websites directed at children or who have actual knowledge that particular users are children must undertake the costly process of obtaining verifiable parental consent. If they do not, they must either cripple the functionality of their website or implement monitoring functions that would prevent children from making any personally identifiable information available online.

---

[8] *See, e.g.* Facebook.com, Statement of Rights and Responsibilities, http://www.facebook.com/terms.php?ref=pf (last visited June 30, 2010) ("You will not use Facebook if you are under 13."); Google Terms of Service, http://www.google.com/accounts/TOS?hl=en (last visited June 30, 2010) (requiring users be of legal age to form binding contract to use services); Myspace.com, Terms & Conditions, http://www.myspace.com/index.cfm?fuseaction=misc.terms ("By using the MySpace Services, you represent and warrant that… you are 13 years of age or older).

[9] Popular sites generally stick to using one of the enumerated verification methods, like "email plus". *See, e.g.*, LiveJournal Privacy Policy, http://www.livejournal.com/legal/privacy.bml (last visited June 30, 2010) (using an "email plus" authorization); Club Penguin, http://www.clubpenguin.com (last visited June 30, 2010) (using an "email plus" verification).

[10] In 2007, the Commission found that no changes were necessary to COPPA because it had been "effective in helping to protect the privacy and safety of young children online." *2007 COPPA Implementation Report*, *supra* note 3.

[11] *See* Joint Comments 3.

VI. Question 3c: What changes should be made to the Rule?

While, as noted, there are costs associated with compliance with the Rule, the balancing judgment that Congress made in enacting COPPA is not unreasonable. If the Rule continues to be focused as it is on specific types of contacts with children under 13, the balance struck continues to be appropriate.

VII. Question 5: Are there any overlaps or conflicts with other federal, state, or local government laws or regulations, or gaps where no law or regulation has addressed an issue relating to children's online privacy?

A number of states have attempted or succeeded in passing laws that would extend COPPA-like restrictions on the collection of information from children to cover older minors;[12] these efforts have generally failed to pass or have been struck down as unconstitutional.[13] While neither state nor federal attempts to expand COPPA to cover older minors would pass constitutional muster,[14] the threats to children's online privacy can be addressed under existing law. As we recommend in our Joint Comments, the Commission should work with state Attorneys General to increase state enforcement of COPPA and to prosecute operators who violate the law.[15] State and federal unfair and deceptive trade practice law can also be used to prosecute advertisers who target children with false claims in advertisements.

---

[12] Bills in both North Carolina and Georgia requiring parental consent for all minors on social networking sites failed to pass. *See* S.B. 132, 2007 Gen. Assem., Reg. Sess. § 8 (N.C. 2007), *available at* www.ncga.state.nc.us/Sessions/2007/Bills/Senate/HTML/S132v3.html (original version of bill requiring parental permission for minors to access commercial social networking Web sites did not pass); 2007 N.C. Sess. Laws 2008-218 (2007), *available at* *http://mainelegislature.org/legis/bills/bills_124th/chapters/PUBLIC230.asp* (bill eventually passed without parental permission requirement); S.B. 59, Gen. Assem., 2007-2008 Leg. Sess. (Ga. 2007), *available at* www.legis.ga.gov/legis/2007_08/fulltext/sb59.htm. A similar bill was proposed in 2008 in New Jersey, but has not made it out of committee. *See* A.B. 108, Gen. Assem., 213th Leg. Sess. (N.J. 2008), *available at* www.njleg.state.nj.us/2008/Bills/A0500/108_I1.HTM

[13] In a recent effort, Maine attempted to pass a marketing-to-minors law that prohibited collection of personal and health-related information from minors without verifiable parental consent and prohibited the transfer, online or offline, of any information about Maine minors, even with parental consent. SP0431, 2009 Leg., 124th Sess. (Me. 2009), *available at* http://mainelegislature.org/legis/bills/bills_124th/chappdfs/PUBLIC230.pdf. This law went beyond COPPA in violation of the First Amendment rights of minors. After Maine Attorney General Janet T. Mills pledged not to enforce the problematic law, the state legislature repealed it in March 2010. *See* Justin Ellis, *Online Privacy Statute Sent Back to Lawmakers*, Portland Press Herald, March 4, 2010, *available at* http://www.pressherald.com/archive/online-privacy-statute-sent-back-to-lawmakers_2009-09-08.html ("Attorney General Janet Mills "acknowledged her concerns over the substantial overbreadth of the statute and the implications of (the law) on the exercise of First Amendment Rights and accordingly has committed not to enforce it.'"); SP0649, 2010 Leg., 124th Sess. (Me. 2010), *available at* http://mainelegislature.org/legis/bills/bills_124th/chappdfs/PUBLIC560.pdf (repealing SP0431).

[14] *See* Joint Comments at 7-10 for a full discussion.

[15] *See* Joint Comments at 11.

VIII. Question 6: Do the definitions in 312.2 accomplish COPPA's goals?

a. Child

The definition of "child" as "an individual under the age of 13" focuses the scope of the Rule properly on younger minors and respects Congress's decision to limit the application of COPPA to children twelve and under in order to preserve the First Amendment rights of older minors.

b. Internet

The definition of "Internet" in the statute represents a successful effort by Congress to craft a definition that is device-neutral and will be applicable to the successive iterations of the Internet in the conceivable future. The Rule implements this definition appropriately, which ensures that as new technologies are developed that have the capability to access the Internet, the Rule will apply to these new technologies as it does to those that exist today.

IX. Question 7: Are the definitions in 312.2 clear and appropriate?

a. Operator

With the advent of new technologies for data transmission such as peer-to-peer systems, the Commission should recognize limits on who could be considered an "operator" of an online service. For peer-to-peer systems that lack a central server or data repository, there would likely not be any "operator" of a "website" or "online service" to whom COPPA responsibility could attach. As detailed more fully below under Question 14, a mere creator or distributor of software would not likely be COPPA covered, and in the absence of an "online service" run by an "operator," COPPA may not apply. We are not, however, aware of any peer-to-peer systems "directed to" children or which currently are in broad use by children. Rather than attempting at this time to expand the Rule to reach a hypothetical peer-to-peer system that might in the future be frequently used by children, we urge the Commission to revisit the questions raised should such systems later arise.

X. Question 8: Should the definitions of "collects or collection" be modified in any way? How will the use of centralized authentication methods affect individual websites' COPPA compliance efforts?

"Collects or collection" is defined as "the gathering of any personal information from a child by any means." This definition is more expansive than the common usage of the term and includes "the passive tracking or use of any identifying code linked to an individual, such as a cookie" or anything that "[enables] children to make personal information publicly available through a chat room, message board, or other means." This definition is sufficiently broad to cover the likely methods for acquiring a child's personal information.

While there has not yet been widespread adoption of centralized authentication technologies across the web, growing use of systems such as OpenID may affect individual websites' COPPA compliance obligations. In the Open ID system, the identity

provider maintains the user's account, which includes a username and password, and may include other information.[16] Sites that permit users to use OpenID to log in only receive the username and a confirmation signal from the identity provider that the login information is correct. This confirmation signal is not a type of "personal information" under the current Rule and should not be added to that definition as it does not permit the physical or online contacting of an individual. A site accepting an OpenID login may face COPPA compliance obligations due to their receipt of the username from the identity provider, but this is not unique to the OpenID context; usernames that permit the online contacting of an individual are already covered under the Rule's definition of "personal information."[17]

XI. Question 11: What are the implications for COPPA raised by mobile communications, interactive television, interactive gaming, or interactive media?

The Rule's definition of "Internet" covers the transmission of data via TCP/IP regardless of the device being used. Mobile communications and interactive gaming applications that use the Internet to transmit data are properly considered "online services" under the Rule, and operators of such services must comply with COPPA's regulations.

Some gaming devices, however, enable interactive gaming that does not occur via the Internet, but rather by using local wireless networks that create a connection between the devices. A local Wi-Fi or Bluetooth network is not part of the "interconnected world-wide network of networks," and the information transmitted across such networks should not be covered by COPPA. COPPA is concerned with unauthorized collection of children's information, and the potential for this information to be used to inappropriately contact the child. On the Internet at large, and without COPPA's regulations in place, it can be difficult for parents to know when and by whom information about their children is being collected. But the networks created by these mobile or gaming devices are "local" in the physical sense, requiring members of the network be within 100 meters of each other. The privacy and safety concerns for children are quite different when the reach of the network they are using is so limited, and the potential for collection of personal information of the type COPPA is designed to prevent is greatly reduced.

XII. Question 12: Do the items currently enumerated in the definition of "personal information" need to be clarified or modified?

The items enumerated in the Rule as "individually identifiable information" are clearly described and are reasonably included as types of personal information in the Rule's definition. In part (c) of the Rule's definition, the clause concerning "a screen name that reveal's an individual's e-mail address" could be redundant because any screen name that

[16] The operator of the identity provider must of course comply with COPPA, as it is an operator of an online service; depending on what information the identity provider collects for the user's profile (including the user's age), and whether it operates a centralized authentication system "directed to children", the identity provider may need to obtain verifiable parental consent before permitting a child to create a profile.
[17] 16 C.F.R. 312.2(12)(c).

provides a means of contacting an individual would likely fall under "other online contact information" whether or not the screen name included an individual's e-mail address. Thus, for example, a social network identifier would allow an individual to be contacted, and would likely qualify as "online contact information." On the other hand, it is not clear there is a strong need to change the rule to address this possible redundancy.

XIII. Question 13(a): Do operators have the ability to contact a specific individual using one or more pieces of information collected from children online? Are they doing so?

Operators may have the ability to contact an individual online using one or more pieces of information specified in Question 13(a). If an operator collects an instant messaging username from an individual, for example, the operator would likely be able to send that a message to that username; thus, the Rule appropriately includes "instant messaging user identifier" in the definition of "personal information".[18]

XIV. Question 13(b): Should the definition of "personal information" in the Rule be expanded to include any such information?

The definition of "personal information" in the COPPA Rule is narrower than definitions of "personally *identifiable* information" (PII) found in other contexts. CDT generally supports a robust definition of PII, going beyond traditional identifiers to include biometrics, persistent identifiers such as Internet protocol (IP) addresses, preference profiles and other information that could reasonably be associated with an individual. In addition, we believe that certain data – such as location information, medical history, financial information, among other categories – should be viewed as "sensitive" information warranting even greater protection.

But, notwithstanding its relative narrowness, the definition of "personal information" in the COPPA Rule is generally sufficient in light of the specific structure and focus of the COPPA requirements. The COPPA definition focuses on information that will permit not just the identification but also the physical or online *contacting* of a child, and the statute places constraints on the bare collection (as opposed to use) of "personal information." The broader and more inclusive definitions of PII are appropriate in their contexts, but are not essential to achieve the purposes of COPPA (and at least some situations, as discussed immediately below, a broader definition of "personal information" in the COPPA context could be harmful to normal Internet communications).

The Commission seeks comment on a number of specific categories of information, three of which we address:

IP Addresses: The Commission asks whether the definition of "personal information" should be expanded to include IP addresses. Although CDT believes that IP addresses would appropriately be included in a broader conception of PII, including such addresses in the COPPA scheme would cause significant problems. COPPA prohibits the *collection* of personal information from children. This sets COPPA apart from other pro-

[18] 16 C.F.R. 312.2(12)(c).

consumer privacy regulations and proposed statutes, which define PII to include IP address data and which commonly regulate the *use* of such PII. While it is accurate and appropriate to treat a persistent IP address as data that could be used to identify an individual (or at least a particular device), a prohibition on the mere collection of this data would undermine the very functioning of the Internet. Every time any user accesses a website or uses an online service – even for the very first time – the server that hosts the site or service receives the user's IP address. If this transmittal of IP address were considered "collection of personal information" under COPPA (as it would for, for example, the operator of a site aimed at children), then as soon as a child attempted to access a site or service directed to children, the operator would be collecting personal information, without any opportunity to first obtain parental consent for the collection. In other words, even before a site operator had a chance to obtain parental contact information in order to comply with COPPA, the operator would already have violated COPPA. The Commission should continue to monitor the potential for inappropriate uses of IP address information (in both the COPPA and other contexts), but because of the particular function of the COPPA Rule, IP address should not be included in the Rule's definition of "personal information".

Behavioral advertising information: The Commission also asks whether information collected in connection with online behavioral advertising should be included in the Rule's definition of "personal information." The issue of collection of children's information through online behavioral advertising networks is important, and has been examined both by advertisers and the Commission itself. Industry groups have released several sets of self-regulatory principles concerning behavioral advertising, each of which prohibits the collection of information about children without parental consent.[19] In addition, the Commission's own Behavioral Advertising Guidelines classifies information about children as a category of "sensitive" information that should not be collected by behavioral advertising networks.[20] Thus, although behavioral advertising information does not cleanly fit within the existing terms of the COPPA Rule, it appears that other initiatives have adequately addressed the concern about such profiling of minors (or minors' families). We urge the Commission to not seek to fit behavioral advertising information into the COPPA Rules at the time, but instead to continue to monitor the uses of profile information on behalf of all users, and to consider further action should advertisers fail to live up to their commitment not to collect such information from children.

---

[19] Network Advertising Initiative, *2008 NAI Principles Code of Conduct* 9 (Dec. 16, 2008) ("Use of non-PII or PII to create an OBA segment specifically targeting children under 13 is prohibited without verifiable parental consent. . . . This standard incorporates by reference the definition of "child" established in the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C § 6501 et seq. NAI members relying on children's PII should refer to CARU guidelines even for contextual ad selection, which remains unaffected by this provision. Where children's PII can be used to tailor ads through non-contextual OBA or Multi-Site advertising services, the prohibition of Section III.4(a) shall not apply where the member can obtain verifiable parental consent, as defined by COPPA."), *available at* http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Web; Interactive Advertising Bureau, *Self-Regulatory Principles for Online Behavioral Advertising* (July 1, 2009) ("Entities should not collect "personal information", as defined in the Children's Online Privacy Protection Act ("COPPA"), from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for Online Behavioral Advertising, or engage in Online Behavioral Advertising directed to children they have actual knowledge are under the age of 13 except as compliant with the COPPA."), *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf

[20] FTC, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 10 (2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

Location information: One type of information the Commission should consider adding to the Rule's list of "individually identifiable information" is geolocation information.[21] Mobile applications often include precise location information when transmitting data back to an online service.[22] This type of location information can pinpoint a person's whereabouts relative to the nearest cell tower, or even the exact latitude and longitude of the mobile device.[23] Because the majority of people spend most of their time in two locations – in the case of children, at home or at school – mobile geolocation data can reveal highly specific personal information about an individual's habits and location, including a probable place of residence.[24] Moreover, it is now a technically trivial matter to "reverse geocode" a location to convert (for example) a latitude and longitude into a street address, which can then be used to contact an individual.[25] The Rule prohibits the collection and use, without parental consent, of exactly this type of information, and the Commission should update the definition of "personal information" to clarify that geolocation information is included.

XV. Question 14: Are providers of downloadable software collecting information from children that permits the physical or online contacting of a specific individual?

There are a number of ways to interpret this question, but however interpreted, the basic answers are "it depends" and "it does not really matter under COPPA." This question could be asking about operators of services that sell or distribute software (which could be anyone from Amazon.com to an Android-focused "App Store"). There is nothing inherent in the transaction of downloading software that involves collecting information from children that permits the physical or online contacting of a specific individual. A website or online service that provides downloadable software may or may not collect information (just as any website or online service may or may not collect information).

---

[21] The Commission's question asks about *mobile* geolocation information, but the Commission should not limit its consideration of location information to the mobile context. Although mobile location applications and services are certainly garnering current attention, location-based services are in no way confined to mobile applications. Such services are equally applicable to both nomadic and fixed online line access, and the privacy risks (to both minors and adults) can be even greater with the use of location-identifying services in the non-mobile context.

[22] For example, the Google Search for mobile application allows you to search for nearby places without typing in your location by using location information from your mobile device. Google Search for Your Phone, http://www.google.com/mobile/search/ (last visited June 30, 2010).

[23] Google Latitude, using technology available to any application, can use Wi-Fi networks to find location within 200 meters; multiple cell towers to get within 100 meters; or GPS networks to get within a few meters. Steven J. Vaughan-Nicholas, *FAQ: How Google Latitude Locates You*, ComputerWorld, Feb. 5, 2009, http://www.computerworld.com/s/article/9127462/FAQ_How_Google_Latitude_locates_you_.

[24] A study by Microsoft research showed that using GPS tracks from a vehicle and heuristic algorithms made identification of home location possible. JOHN KRUMM, INFERENCE ATTACKS ON LOCATION TRACKS, PROCEEDINGS OF THE 5TH INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING 127 (2007), *available at* http://research.microsoft.com/en-us/um/people/jckrumm/Publications%202007/inference%20attack%20refined02%20distribute.pdf. Using GPS coordinates, the study was able to look up the identity of the individual using Web based white pages. *Id.* While his study only correctly identified an individual approximate five percent of the time, in the case of mobile data, the accuracy would be even higher as the mobile device would actually be used within the house rather than a car, which may be parked in different locations. *Id.*

[25] *See, e.g.,* http://code.google.com/apis/maps/documentation/geocoding/

Certainly any vendor who *sells* software is likely to collect information as part of the transaction, but online sites like Download.com make free and trial software available without collecting personal information from the recipient. In any event, the operator of an online software store or an "App Store" would almost certainly fall under the COPPA definitions of "website" or "online service," and thus depending on other factors they may well be covered by COPPA (and would be covered without any changes in COPPA or the COPPA Rule).

This question may also be asking about the implications of software that, once downloaded, collects and transmits information to another person or entity. In this case, the Commission should be clear that the designer or maker of the software would not incur obligations under COPPA (because standing alone, the software is neither a website nor an online service), but that if a piece of software transmits information back to a particular person or entity online, the recipient of the information could well be covered by COPPA as an "online service." Thus, if an independent app maker designs a piece of software to (for example) interact with and transmit information to a service like Twitter, then the software maker is not covered by COPPA, but the operator of the online service might well (depending on other factors) be covered by COPPA. If it happens that the operator of an online service *also* provides a piece of client software to access the service, then the "provider" of the software might well be covered by COPPA, but their obligations arise from their activities as an operator of an online service, and *not* because they distributed a piece of software.

The Commission should focus its attention, as the COPPA statute requires, on the operators of websites and online services, and not on the designers or distributors of software that can interact with such services. To restate the point in a specific context, just because one can access COPPA-covered services using a web browser does not mean that the designer or distributor of the browser (such as Mozilla or Microsoft) has any COPPA obligations that arise because of users' use of the browser.

* * *

We appreciate the opportunity to comment on the important questions raised in the RFC, and we look forward to working further with the Commission as it continues its COPPA review.

Respectfully submitted,

John B. Morris, Jr
Emma J. Llansó
Mangesh Kulkarni
Center for Democracy & Technology
1634 I Street, NW, Suite 1100
Washington, DC 20006
(202) 637-9800

June 30, 2010