



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

June 30, 2010

FILED ELECTRONICALLY

Federal Trade Commission

In the Matter of COPPA Rule Review, P104503

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 in further detail below, NetChoice believes that the COPPA rules generally work well to serve the interests of children, parents and online companies. Our comments reflect recent experiences in state legislatures with proposed legislation that would contradict and expand COPPA.

NetChoice is a coalition of trade associations and e-commerce companies, plus over 13,000 small businesses that rely on e-commerce. NetChoice works to promote the integrity and availability of the global Internet, and 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 four specific areas, and ask that the Commission:

1. Maintain the current age threshold at twelve years and under
2. Retain the "actual knowledge" standard
3. Clarify that states may not enact laws that conflict with COPPA
4. Conclude that geolocation & IP Address data are not individually identifiable information, and that COPPA already applies to the mobile Internet

In the next sections, we discuss the continuing need to keep key aspects of the rule in its current form, including the current age threshold and knowledge standard.

1. Maintain the Current Age Threshold at Twelve Years and Under

One of the key aspects of COPPA's success is that it applies to a well-defined demographic— young children under the age of 13. As opposed to teenagers, younger children are not as active on the Internet and have distinct tastes, preferences, and aptitude levels. It is therefore easier to determine whether a website is directed to young children than it is to assess whether sites are directed to teenagers, who share interests, aptitude, and abilities more in common with adults.

Yet, at the Commission's COPPA Rule Review roundtable event, we heard participants advocate for increasing COPPA's scope to cover teenagers. Some think that there's an adolescent "gap" that should be addressed. Even if the Commission were inclined and had the authority to increase the age of applicability for COPPA, Congress specifically selected children under 13 as deserving of special attention. And COPPA is not alone with identifying age 13 as a milestone :

- The Federal Communications Commission defined "children" as *under the age of 13* for purposes of the Children's Television Act.
- MPA movie ratings – PG 13 ("Parents strongly cautioned—some material may be inappropriate for children under 13").
- Entertainment Software Rating Board computer and video game ratings – T ("Teen") rating indicates that content "may be suitable for ages 13 and older."
- Internet Education Foundation Parental Empowerment and Convergence Guide – 13 is threshold age for exposure to more mature movies, TV programs and computer/video games.

Increasing COPPA's age threshold to age 15 or even 17, for instance, would be a wrongheaded approach. It would greatly expand COPPA's reach and create new liability for thousands of websites. It could also force sites to age verify and obtain parental consent on a massive scale. Yet, we know that is impossible to precisely determine a child's age online. According to a report of Harvard University's Berkman Center, "*age verification and identity authentication technologies are appealing in concept but challenged in terms of effectiveness.*"¹

There are practical problems of parental verification on a widespread scale. Verifiable parental consent is difficult to implement, and many sites simply lock-out their websites to anyone indicating they are under 13 years old.² However, a simple COPPA lock-out won't easily translate to the 13 to 17 age bracket affected by this Act, as teenagers are more adept at circumventing online locks of any kind. And because it requires involvement by parents, relying on parental verification may not protect society's most vulnerable minors who have absentee parents.

¹ Available at <http://cyber.law.harvard.edu/pubrelease/isttf/>

² Berin Szoka and Adam Thierer, COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech, Progress & Freedom Foundation, available at <http://www.pff.org/issues-pubs/pops/2009/pop16.11-COPPA-and-age-verification.pdf>

In addition, there are privacy and security concerns related to age verification methods. After all, the process of verifying age necessarily entails the collection of data sufficient to determine proof of age, and all this data must be transmitted, processed, and stored. Finally, it should be recognized that Congress chose not to apply COPPA's parental consent regime to teenagers because of free speech concerns. In many circumstances, such as access to reproductive health information, adolescents have First Amendment rights on par with adults. Therefore, the rights of 13 to 17 year olds to access and receive information are stronger than those of younger children.

2. Retain the “Actual” in the “Actual Knowledge” Standard

COPPA applies when a website is directed to children. But COPPA also applies when a website operator that has “actual knowledge that it is collecting personal information from a child” from children 12 and under. In any new COPPA rules, the Commission should maintain a strict construction of what it means to have “actual knowledge” and apply COPPA when website operators know *in-fact* that they have collected information from children.

The COPPA rule does not define “actual knowledge.” Generally, it is viewed as a heightened requirement for a mental state of possessing information. In the context of COPPA, “actual knowledge” would apply when a site learns a child's age by asking for and receiving information from which it can determine age.

The “actual knowledge” standard is an important one for continued innovation on the Internet and for the future of user-generated content. It ensures that only culpable actors—sites that know they're collecting information on children—are held liable for violating COPPA. At the same time, it prevents regulators from piecing together bits of information and determining on their own that a site should have known it was collecting information from children.

At the Commission's COPPA Rule Review roundtable, we heard panelists describe how Congress initially considered a lower “knowingly” standard. This standard would have imposed a “should've known” obligation. A “knowingly” standard is more akin to a “constructive knowledge” standard, not *actual* knowledge. It would burden websites into mining data, to be sure that they would not be accused that they *should've* known.

COPPA compliance should not be a matter of *shoulda*, *woulda*, *coulda*. The Commission should reinforce its commitment to enforce the actual knowledge standard in ways that will not innocently trip up website operators.

Next, we describe state legislative attempts that would overlap and conflict with COPPA, including our on-the-ground experiences with proposed legislation.

3. Clarify that States May Not Enact Laws that Conflict with COPPA

COPPA works well because it sets a national standard, preventing states from enacting similar laws that would impair interstate commerce. As Internet commerce knows no borders, online companies have had to work vigorously to keep state laws roughly consistent when it comes to

information privacy. COPPA serves an important purpose by preventing an unworkable patchwork of inconsistent state laws.

However, states are increasingly proposing legislation that would regulate Internet communications and information collection in ways that would conflict with COPPA. The past few years have seen a number of state proposals to regulate child privacy in ways that would conflict with COPPA.

States have proposed legislation to regulate how information from and about minors can be collected, used and shared. In addition, states have looked to apply parental verification requirements beyond COPPA's limited scope.

Proposals to Regulate Information Collection

For example, NetChoice was a lead plaintiff in a lawsuit challenging a Maine law that placed broad restrictions on the collection and transfer of personal information about minors. The law, passed in 2009, required websites to obtain "verifiable parental consent" before collecting personal data or marketing to Maine teens under the age of eighteen.

As a result of the lawsuit, Maine's Attorney General agreed not to enforce the law, pending revision or repeal by the legislature. As a result, the legislature organized a two-day joint hearing of the judiciary committee where NetChoice and a number of affected companies filed comments and traveled to Augusta to testify.³ Our goal: persuade the committee to recommend full repeal of the law.

A large part of our argument was that the proposed law conflicted with COPPA. Because the bill applied to children under age 13, it was in direct conflict. Furthermore, because it extended COPPA's reach to teenagers up to age 17, it conflicted with Congress's informed decision to limit COPPA's rule to children 12 and under.

Earlier this year, Maine's Senate took-up legislation to repeal the law, but added replacement language focused on medical products and services. The new language would have required verifiable parental consent for showing ads relating to any health concern. Eventually, the sponsor dropped her replacement language and the legislature repealed the marketing to minors law.

NetChoice has also opposed online safety-related legislation that would have had serious privacy implications. Last year, New Jersey proposed a law to extend COPPA's requirements from children twelve and younger to include teens up to 17 years old.⁴ As is the case under COPPA, Internet services and Web sites would have been required to obtain verifiable parental consent when attempting to collect personal information from teenagers in addition to children twelve and under.

³ See <http://www.maine.gov/legis/opla/judcommreview.htm>

⁴ 213th Legislature, Reg. Sess. (N.J. 2008), available at http://www.njleg.state.nj.us/2008/Bills/A0500/108_I1.PDF

The bill would have extended COPPA's reach to apply to all Internet websites *directed at adolescents* and dramatically altered the innovative landscape of online services. It would have effectively required parental consent before any teenager could obtain an e-mail address, Instant Message address or register to receive information from a website. It would also have clearly applied to many social networking websites.

The bill was withdrawn by its sponsors before it could be heard in committee, after a groundswell of opposition from child safety experts, public interest groups, legal experts, and industry.

Proposals to Require Parental Verification

Another variation of COPPA-like state legislation would apply only to social networking websites. These bills required parental consent before a minor can become a registered user of a social networking website. Variants of this requirement were introduced in Connecticut, Georgia, Mississippi and North Carolina in 2007 or 2008, and in Illinois last year.⁵

The typical bill language used to create a duty on social networking websites to obtain verifiable parental consent goes something like this:

No owner or operator of a commercial social networking website shall allow a minor using a protected computer to create or maintain a personal webpage on a social networking website without first obtaining the permission of the minor's parent or guardian and without providing the parent or guardian access to the personal webpage at all times the commercial social networking website is operational.

The typical bill language used to create a duty to authenticate age and parental identity is as follows:

Any owner or operator of a social networking website shall adopt and implement procedures to confirm the identity and age of parents or guardians who are providing permission for their minor children and members at the time of registration by validating the accuracy of personal identification information submitted at the time of registration.

Finally, social networking websites would have to retain permission records, perhaps indefinitely:

The owner or operator of a social networking website must keep either a hard copy or electronically scanned copy of the written permission of the parents or guardians in a database maintained by the social networking website.

NetChoice worked with other members of the online community to present the privacy pitfalls involved with collecting and keeping additional personal information just in order to comply with new legislation. To verify parental consent, for example, online services must require

⁵ H.B. 6981 (Conn. 2007), S.B. 59 (Ga. 2008), S.B. 2586 (Miss. 2008), S.B. 132 (N.C. 2008), HB 1312 (Ill. 2009).

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.

As well-intentioned as some of these bills may seem, compliance with state law by operators of websites available nationally (and internationally) is difficult, burdensome and costly. 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...*"⁶

As mentioned above, state laws that regulate the online collection of information from children do not yet present insurmountable compliance barriers. However, the Commission should be aware of state activity and intervene where appropriate to help prevent a patchwork problem for interstate e-commerce. The Commission should consider communicating with state attorneys general and legislators about potential conflict with COPPA.

4. New Rules are Not Needed for Geolocation, IP addresses, and the Mobile Internet

Finally, we believe that the Commission should specify that geolocation and IP address data are not individually identifiable information, and that COPPA already applies to the mobile Internet.

The COPPA Rules should reflect that geolocation data and IP addresses are not, by themselves, individually identifiable information. Geolocation informs where a device is physically present, but it does not necessarily inform who possesses the device. Likewise, IP addresses identify *devices* on a computer network, not *people*. However, when combined with name, address or social security number data, geolocation and IP address information "gets personal" and becomes personal information as defined by COPPA.

Furthermore, the Commission should conclude that mobile Internet already falls within COPPA's rules. COPPA is device agnostic—it does not matter whether a device is mobile, plugged in, or sitting on a desktop, if it's on the Internet then COPPA applies.

We believe that new rules are not needed for geolocation, IP address, and the mobile Internet. However, if the Commission determined it should proceed with a rulemaking in these specific areas, it could do so without Congressional involvement. When Congress passed COPPA, it specifically provided the FTC with APA rulemaking authority to implement the Act. The FTC thus has latitude to ensure that the Act remains relevant in today's online world, so long as it does not expand COPPA beyond the scope of Congressional intent.

⁶ 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/>

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Steve DelBianco", with a long horizontal flourish extending to the right.

Steve DelBianco
Executive Director

A handwritten signature in black ink, appearing to read "Braden Cox", with a long horizontal flourish extending to the right.

Braden Cox
Policy Counsel

NetChoice is a coalition of trade associations and e-Commerce businesses who share the goal of promoting convenience, choice and commerce on the Net. More information about NetChoice can be found at www.netchoice.org