Before the
Federal Trade Commission
Washington, D.C.

COPPA Rule Review	)	Project No. P104503
	)	
16 CFR Part 312	)	
_____	)	

COMMENTS OF COMMON SENSE MEDIA

The Federal Trade Commission's proposals for the Children's Online Privacy Protection Act Rule are critical steps toward helping the COPPA law keep pace with rapid changes in the online and mobile worlds and maintaining the law's core purpose: helping parents protect their children – and their fundamental right to privacy – online. Put simply, children's online information should not be collected, used, or shared – and children should not be tracked online – without consent from a parent or guardian.

This basic principle was true when the law was passed by a bipartisan majority in Congress in 1998, and it's even more true today, as online tracking and data collection continue to grow at an ever-increasing pace. There can be no question that the online and mobile worlds that surround our children today have an enormous effect on their social, emotional, and cognitive development. As Common Sense Media founder James P. Steyer recently wrote, "The last time we seriously examined our nation's privacy laws, Facebook founder Mark Zuckerberg

was still in grade school, and YouTube, text messaging, and Twitter didn't exist."[1] Major new advances in privacy protection for kids are absolutely essential.

The Commission's important updates address social media platforms and other recent innovations in technology. Equally important, the revisions meet the fundamental goal of COPPA – helping parents and guardians maintain their traditional role as the primary gatekeepers in young children's lives.

Common Sense Media is a nationally respected nonprofit, nonpartisan organization dedicated to providing parents, educators, kids, and others with tools and information to help them make smart choices about the tremendous opportunities – and potential pitfalls – in the world of digital media. Each year, we work with tens of millions of parents and tens of thousands of educators and schools, as well as media and technology companies and policymakers at the local, state, and national level. Because of our work with each of these groups, we very clearly recognize why these COPPA updates – and the careful balance the Commission has drawn – matter to all key stakeholders. For example:

- Updated online privacy protections matter to parents. Parents want their children to access the benefits of the Internet and digital media and also want to continue their parental role of deciding which digital media – and which online and mobile interactions – are an appropriate fit for their children and respect their children's fundamental right to privacy.
- Updated online privacy protections matter a great deal to education because they point toward a crucial balance in which students can explore new e-learning opportunities – in

[1] "Talking Back to Facebook," James P. Steyer, 2012

school, at home, and in between – but also have protections for their personal information as they learn to manage their own digital reputation.

- Equally important, updated online privacy protections matter enormously to innovation in e-learning and e-commerce. Rules that help ensure that young children's information is protected – and the role of parents and guardians is respected – will maintain and expand online environments that parents and teachers can trust. Trusted environments are key to the ongoing growth and success of e-learning and e-commerce. Respecting parents and their role in protecting their children isn't a barrier to innovation; indeed, it represents an essential component of innovation that *works* – for kids and families, for online and mobile companies and developers, and for our nation as a whole.

I. Clarifying Responsibilities of Social Networking Services and Other Plugins on Sites Directed at Children.

Common Sense Media agrees with the goal of clarifying that both child-directed sites and services and information-collecting sites and services are responsible covered co-operators. The data collectors and those who technically enable collection should be responsible for their technologies. The burden should not fall on parents and kids to decipher the rapidly changing technologies used to track online behavior, especially when those technologies often seem to be designed to be difficult to understand.[2]

[2] "Our work demonstrates that advertisers use new, relatively unknown technologies to track people, specifically because consumers have not heard of these techniques. Further, these technologies obviate choice mechanisms that consumers exercise." Hoofnagle, Chris Jay, Soltani, Ashkan, Good, Nathan, Wambach, Dietrich James and Ayenson, Mika, *Behavioral Advertising: The Offer You Cannot Refuse* (August 28, 2012). 6 Harvard Law & Policy Review 273 (2012). Available at SSRN: http://ssrn.com/abstract=2137601

a. Operators who add plugins and other functionality should be responsible for the data collection they enable.

Common Sense Media supports placing this responsibility on operators of online services, rather than leaving parents and families to identify all the potential third-party data collectors on the online service(s) they seek to use.

COPPA includes as covered operators both those who collect personal information and those who have personal information collected on their behalf. The Commission proposes to cover operators who integrate third-party plugins by introducing a definition for the term "collected or maintained on behalf of" an operator.

> Personal information is *collected or maintained on behalf of* an operator where it is collected in the interest of, as a representative or, or for the benefit of, the operator. [3]

Thus sites which do not collect personal information, but have plugins that do, will be deemed covered operators.

The proposed language could use some clarification, as Common Sense Media is concerned that the proposed definition may be read too narrowly. For example, an advertising network collects information primarily for its own benefit, and the benefit that the original site or service receives is secondary. The Commission should clarify that this secondary benefit is also "for the benefit of the operator" and that advertising networks and similar operators are covered.

Secondly, the original operators may claim they are unaware that benefits – if any – flow from data collection. Opposing commenters may make a similar argument against the rule: That an operator should not be covered solely because third parties are collecting data on that

[3] Children's Online Privacy Protection Rule; Supplemental Notice of Proposed Rulemaking, 77 Fed. Reg. 46,643 46,644 (August 6, 2012), available at www.ftc.gov/os/2012/08/120801copparule.pdf.

operator's site, and that it would be too difficult to determine the extent of the data collection. These arguments should be rejected.

Operators should be responsible for the data collection mechanisms on their sites or services. Parents and children should not be the ones required to investigate the presence and data collection practices of plugins or third parties on the site(s) they wish to use. Nearly two years ago, *The Wall Street Journal* found that 30% more tracking cookies and beacons were placed on a test computer by sites popular with children and teens, compared to general audience sites.[4] A more recent report from *The Wall Street Journal* highlighted how mobile games and apps are increasingly popular – for young kids and also for marketers aiming to reach them.[5] This is not a problem created by parents and not a problem that parents should be expected to decipher or solve.

Operators may claim that it is too difficult to understand how their plugins collect data or what the proper disclosures should be. But perspective is essential here: If *operators* feel their relationships with third parties are complex, clearly those relationships will be even more complex to parents and families. When Congress passed COPPA with strong bipartisan support in 1998, they made the policy choice clear. It is not parents who are responsible for uncovering data collection practices. It is the operators of sites directed at children who must disclose their practices and get verified parental consent for collecting children's data. Further, as the Commission notes, the liability is premised on the fact that operators benefit from the presence of these plugins. It is fair that this benefit come with some responsibility.

---

[4] Steve Stecklow, *On the Web, Children Face Intensive Tracking*, The Wall Street Journal, Sept. 17, 2010, http://online.wsj.com/article/SB10001424052748703904304575497903523187146.html.

[5] "The mobile games demonstrate how new technology is changing U.S. commerce, drawing tighter bonds between marketers and young consumers. 'The apps are certainly targeted at kids,' said Melinda Champion, vice president of marketing at J&J Snack Foods Corp." Anton Troianovski, *Child's Play: Food Makers Hook Kids on Mobile Games*, The Wall Street Journal, Sept. 17, 2012, http://online.wsj.com/article/SB10000872396390444812704577605263654758948.html.

As importantly, in its 1999 COPPA rulemaking, the Commission declared that the "proposed Rule's definition of 'Internet' made clear that it applied to the Internet in its current form *and to any conceivable successor*. Given that the technology used to provide access to the Internet will evolve over time, it is imperative that the Rule not limit itself to current access mechanisms."[6] The technology of Internet access certainly has changed – and so have the technologies for collection of personal information. The Commission's proposed Rule changes reflect those changes and wisely update the Rule to keep pace with them.

b. Plugin Providers and Advertising Networks on Child-Directed Sites.

The Commission proposes to cover plugin providers under COPPA if they know or have reason to know that they are collecting information from a site directed at children.[7] The Commission further notes that this is not "intended to impose a duty to ascertain unknown facts."

Common Sense Media agrees that plugin providers should have responsibilities under COPPA. Beyond the Commission's proposal, plugin providers should have at least a minimal duty to inquire whether their plugins are being used by operators directed at children. The duty does not have to be immediate nor a pre-requisite to any data collection. But at least some affirmative steps should be required so that plugin providers are not mere passive collectors of children's data.

As noted above, the plugin providers benefit from this data collection and should bear some responsibility for ensuring that their data collection respects parental autonomy.

[6] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,891 (Nov. 3, 1999), available at www.ftc.gov/os/1999/10/64fr59888.pdf

[7] Children's Online Privacy Protection Rule; Supplemental Notice of Proposed Rulemaking, 77 Fed. Reg. 46,643 46,645 (August 6, 2012), available at www.ftc.gov/os/2012/08/120801copparule.pdf.

II. Screen and User Names as Personal Information

Common Sense Media supports the Commission's proposals to include screen and user names as personal information. The Commission proposes to include screen and user names when they rise to a level of online contact information. These changes reflect the simple observation that online contact can now be achieved via several methods besides electronic mail. Users may chat, tweet, send BlackBerry and Facebook messages, and use various platforms and protocols to contact each other. Various online forums permit users to contact each other via personal message, or "pm."[8] On the Facebook social network, users can "tag" other users in content, causing them to be contacted.[9] Such a feature should be included as contact information – even though in Facebook's case the "screen name" is already an individual's name.

Further, screen and user names can be used to build profiles on individuals outside of the internal operations of a website or online service. For example, the social networking aggregator Spokeo permits users to search by "username."[10] The service skims data from social networking services and compiles it into profiles.[11] Screen or user names that are displayed to non-users of the service and can be used for such profiling should be covered as personal information.

III. Persistent Identifiers

The Commission also proposes to change when persistent identifiers are considered personal information and to change the definition of the "internal operations" operations exception. The proposal would exclude persistent identifiers used for the following purposes:

---

[8] See, eg, phpBB, Communicate with Privacy Messages, http://www.phpbb.com/support/documentation/3.0/userguide/user_pm.php.

[9] Tom Ochino, *Tag Friends in Your Status and Post,* The Facebook Blog, Sept. 10, 2009, https://www.facebook.com/blog.php?post=109765592130.

[10] Spokeo Username Search, http://www.spokeo.com/username-search/.

[11] Cyrus Nemati, *SpokeNo,* Center for Democracy and Technology, July 1, 2010, www.cdt.org/blogs/cyrus-nemati/spokeno.

> (a) Maintain or analyze the functioning of the Web site or online service; (b) perform network communications; (c) authenticate users of, or personalize the content on, the Web site or online service; (d) serve contextual advertising on the Web site or online service; (e) protect the security or integrity of the user, Web site, or online service; or (f) fulfill a request of a child as permitted by '' 312.5(c)(3) and (4); so long as the information collected for the activities listed in (a)–(f) is not used or disclosed to contact a specific individual or for any other purpose.[12]

Common Sense Media supports maintaining persistent identifiers as COPPA personal information. However, the limitation allowing contextual advertising should be limited to first parties. Contextual advertising should be considered "internal" only when done by a first party. If the contextual advertising is done by other operators – such as the plugin providers and advertising networks described in section I – then the use of persistent identifiers can no longer be considered "internal" to the first party.

The Commission has received comments arguing that persistent identifiers merely identify a device, not a user. However, in our increasingly mobile world, a device is increasingly linked exclusively to an individual, and identifying a device is de facto identifying its user. Further, other COPPA personal information has the same properties. For example, in 1998, COPPA covered telephone numbers – which identify devices today and, in 1998, a whole household. Further, COPPA covers an address, which also identifies a household, not an individual.

IV. "Family Sites" Should Enable COPPA Parental Consent

The Commission proposes to change the definition of "directed at children," partially to create a new category of "family sites." Common Sense Media agrees that sites that knowingly target children or that are likely to attract children as a primary audience should be covered by

[12] Children's Online Privacy Protection Rule; Supplemental Notice of Proposed Rulemaking, 77 Fed. Reg. 46,643 46,648 (August 6, 2012), available at www.ftc.gov/os/2012/08/120801copparule.pdf.

COPPA. We also recognize the potential value of this new category and of continuing to enable sites and services to provide materials for children *and* their parents or guardians. Well designed and operated "family sites" could provide parents with better information, and help them be more engaged in their young children's online activities, and would thus serve the spirit as well as the letter of COPPA.

However, this new category of "family sites" may inadvertently create a loophole by allowing services to be widely attractive to kids but to escape COPPA compliance via a simple age gate. This risk can be significantly reduced by requiring these sites to offer parental verification options. Thus Common Sense Media proposes that "family sites" must not only eschew collecting information from those who are under 13 without parental consent, but must also offer the opportunity for parents to consent. Thus we propose that item (c) in the definition of sites "directed at children" be written:

> based on the overall content of the Web site or online service, is likely to attract an audience that includes a disproportionately large percentage of children under age 13 as compared to the percentage of such children in the general population; provided however that such Web site or online service shall not be deemed to be directed to children if it: (i) Does not collect personal information from any visitor prior to collecting age information; ~~and~~ (ii) prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first obtaining verifiable parental consent; *and (iii) actually offers an effective mechanism for obtaining verifiable parental consent prior to any collection of personal information*.

Without requiring that sites offer this mechanism, there is a risk that sites will push the boundaries of what is attractive to kids and will then use a simple age gate to escape liability. If a site is attractive to children, they will have a strong incentive to join. By actually offering a method for providing verifiable parental consent, these "family sites" will go much further toward meeting the goals of COPPA, as well as serving the interests of families.

V. Conclusion

The Commission's COPPA proposals are essential steps to empowering parents and updating protections for children online and for the fundamental right to privacy that we all share. Most importantly, the revisions serve the fundamental purpose of COPPA: helping parents and guardians continue to play their crucial role in protecting the information of their young children.

While the Commission's revisions will update COPPA's protections for children under 13, there are still critically important online privacy concerns for adolescents ages 13 and older, who also need additional privacy protections and strong leadership from both government and industry. We look forward to further action from the Commission to recommend strong and far-reaching protections for teens that address their particular vulnerability to predatory advertising and data collection techniques and that also give them the tools, protections, and educational guidance they need to grow and thrive in this new digital world.

Respectfully submitted,

Alan Simpson

Sept. 23, 2012