

Before the
Federal Trade Commission
Washington, DC

COPPA Rule Review)
)
16 CFR Part 312)
_____)

Project No. P104503

COMMENTS OF COMMON SENSE MEDIA

Summary

The FTC’s proposals for the Children’s Online Privacy Protection Act rule are a significant step in empowering parents and updating protections for children online. 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. The Commission’s updates address social media platforms and other key new technologies that were not present during the initial rulemaking by covering behavioral profiling, location information, VOIP services, screen names, photographs, and video images. The revisions build on the fundamental purpose of COPPA – empowering parents to protect their children's best interests.

Overall, Common Sense Media supports the Commission’s proposals to encourage new methods of parental consent. The data security, retention, and deletion proposals will also protect children’s data from security breaches. While the FTC revisions will keep COPPA’s protections for children under 13 up to date, there are still important online privacy concerns for adolescents ages 13 and older. We look forward to further action and recommendations from the Commission regarding protections for adolescents. Indeed, this represents a critical area of concern for parents and educators, which we strongly believe should be the subject of new national legislation as well as thoughtful regulatory efforts by this and other agencies.

Comments

Common Sense Media is pleased to submit comments in the above-referenced proceeding. Common Sense Media is the nation's leading nonprofit organization dedicated to studying how media impacts children's social, emotional, and cognitive health and to helping children and families thrive in a world of digital media and technology. We offer millions of American families more than 16,000 independent, third party reviews of all types of media and technology content – from movies and video games to websites and mobile applications. We have also created and distributed a free K-12 digital literacy and digital citizenship curriculum to nearly 25,000 schools, which touches on topics raised by COPPA. In addition, we have launched a new state-of-the-art research program focused on media, technology, and children.

I. INTRODUCTION

The FTC's COPPA proposals are a significant step toward updating protections for children online. The FTC's thoughtful and reasoned approach reflects the reality of the present threats to children's privacy and reinforces the role of parents as the primary protectors of their children's emotional and physical well-being.

The proposed revisions will bring COPPA up to date with our rapidly changing and increasingly mobile electronic world. Now more than ever, kids are using mobile devices that enable them to access websites and online platforms and to reveal their personal information, including their precise location. These revisions will also significantly improve protections for children's online privacy, encourage parental involvement, and foster innovation in online services for children. But most importantly, the revisions build on the fundamental purpose of COPPA – to empower parents and guardians to protect their kids' privacy and best interests. As Senator Bryan stated when introducing the Senate version of COPPA:

Senator McCain and I believe there must be safeguards against the online collecting of information from children without a parent's knowledge or consent. If a child answers a phone and starts answering questions, a parent automatically becomes suspicious and asks who they are talking to. When a child is on the Internet, parents often have no knowledge of [with] whom their child is interacting.¹

The FTC has found an important balance in proposing these revisions to keep COPPA's protections for children under 13 up to date. As Chairman Mary Bono Mack said at a recent House Commerce Subcommittee on Commerce, Manufacturing, and Trade hearing on protecting children's privacy in an electronic world:

The purpose of this hearing is to take a close look at the adequacy of existing protections and whether the FTC's proposed changes to COPPA go too far, not far enough, or manage to strike the appropriate balance. Having reviewed these changes carefully, I think the FTC has – as I often say – hit the “sweet spot.”²

However, there are still important online privacy concerns for adolescents ages 13 and older. Common Sense Media looks forward to further strong action from the Commission to recommend protections and education for adolescents, and we also believe that this is an appropriate subject for new national legislation and regulatory efforts.

II. RESEARCH INDICATES GROWING PARENTAL CONCERN AMIDST INCREASED USE OF TECHNOLOGY AND VALIDATES COPPA MODEL OF VERIFIED PARENTAL CONSENT.

Parents are increasingly concerned about online privacy, are significantly dissatisfied with the privacy offerings of major online services, and see a role for policymakers on these issues. In a Common Sense Media/Zogby International poll last fall, 85% of parents said they are more concerned about online privacy than they were five years ago. Further, 61% of parents said that

¹ 144 Cong. Rec. S8483 (July 17, 1998) (Statement of Sen. Bryan).

² PROTECTING CHILDREN'S PRIVACY IN AN ELECTRONIC WORLD: HEARING BEFORE THE SUBCOMM. ON COMMERCE, MANUFACTURING AND TRADE OF THE HOUSE ENERGY AND COMMERCE COMM. (Oct. 5, 2011) (Statement of Rep. Mary Bono Mack), *available at* http://republicans.energycommerce.house.gov/Media/file/Hearings/CMT/100511/Bono_Mack.pdf.

Congress should update laws related to online privacy and security for children and teens.³

Location protections are also heavily supported, as 91% of parents and 81% of teens say search engines and social networking sites should not share their location information without specific authorization.⁴

Equally as important, key new research by Common Sense Media reveals the growing use of digital media by younger children.⁵ Half of all children 8 years old or younger now have access to a mobile device at home.⁶ Slightly more than a quarter of parents have downloaded applications (or apps) for their children to use.⁷ Just over half of 5- to 8-year-olds use a computer more than several times a week.⁸ We include our full report – *Zero to Eight: Children’s Media Use in America* – as an attachment to this filing, as the findings are highly relevant.

Other recent research funded by Microsoft reveals parents’ attitudes about how COPPA is implemented by the social network service Facebook. A vast majority of parents (89%) believe that there “should” be a minimum age to join the service, and the average age suggested by those parents was 14.9 years.⁹ Even larger numbers of parents (93%) believe that they ought to have “final say” about a child’s ability to use an online service.¹⁰ Only a minority of parents (35%) said government should not play a role in determining how websites and online services address children’s use of their services.¹¹

³ Common Sense Media, *Protecting Our Kids’ Privacy in a Digital World*, 1 (Dec. 2010). http://cdn2-www.ec.common sense media.org/sites/default/files/privacy_whitepaper_dec2010.pdf [CSM White Paper].

⁴ *Id.* at 3.

⁵ Common Sense Media, *ZERO TO EIGHT: CHILDREN’S MEDIA USE IN AMERICA* (Fall 2011), available at <http://www.common sense media.org/sites/default/files/research/zerotoeightfinal2011.pdf>.

⁶ *Zero to Eight*, *supra* note 5 at 9.

⁷ *Id.*

⁸ *Id.*

⁹ danah boyd, Eszter Hargittai, Jason Schultz, and John Palfrey, *Why parents help their children lie to Facebook about age: Unintended consequences of the “Children’s Online Privacy Protection Act,”* FIRST MONDAY, Nov. 7 2011, at 12, <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075> [boyd et al.].

¹⁰ *Id.* at 13.

¹¹ *Id.* at 14.

The Microsoft research also showed that, though Facebook chooses not to provide COPPA-compliant access for children under 13, some parents allow children under 13 to create accounts. Sixty-eight percent of parents who knew their child created an account while under age 13 helped them create those accounts.¹² As Commissioner Julie Brill recently described it:

The fact that they are involved in assisting their kids to set up Facebook accounts indicates they want what COPPA seeks to provide – the power to hold their children’s hands as they learn to make choices about how to share data online.¹³

Another recent study from the Pew Internet and American Life Project reinforced why COPPA rules should continue to support and encourage parents’ role. The Pew study found that even teens (ages 12-17) rely most heavily on parents for advice about their online behavior:

- 86% of online and cell-phone using teens say they have received general advice about how to use the Internet responsibly and safely from their parents.
- 58% of teen Internet and cell phone users say their parents have been the biggest influence on what they think is appropriate or inappropriate when using the Internet or a cell phone.¹⁴

Each of these studies reaffirms that parents have concerns about their children’s privacy and try to be involved in protecting that privacy. These studies clearly support the COPPA model of verified parental consent, as well as the need for strong and expanded efforts to protect teens’ best interests.

¹² *Id.* at 9.

¹³ Commissioner Julie Brill, Federal Trade Comm., *Privacy: A Lesson from the Playroom* (Dec. 6, 2011), <http://ftc.gov/speeches/brill/111206iappdraft.pdf>.

¹⁴ Amanda Lenhart et al., *Teens, Kindness, and Cruelty on Social Network Sites*, 6 (Nov. 9, 2011), <http://pewinternet.org/Reports/2011/Teens-and-social-media.aspx>.

III. NO BEHAVIORAL PROFILING OF CHILDREN WITHOUT PARENTAL CONSENT

Common Sense Media has consistently called for limits on behavioral profiling of kids for marketing purposes, and the COPPA updates make clear that behavioral profiling of children should take place only via opt-in parental consent.¹⁵ Common Sense has recommended that all kids not be tracked or have their information transferred to third parties.¹⁶ We have supported limits on behavioral marketing to children and teens.¹⁷ We have also called for the industry-wide adoption of opt-in as the core privacy standard.¹⁸ Common Sense Media is generally supportive of the Commission's proposals and comments to clarify and help the Commission meet these goals.

The new definitions of personal information should not permit tracking by commonly owned online services. The Commission proposes to revise one definition (g) and add another (h).

(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 the website or online service;

(h) an identifier that links the activities of a child across different websites or online services.¹⁹

These definitions cover "persistent identifiers" and the linking of activities across different online services. The definitions are intended to cover behavioral advertising. As the Commission notes:

[T]he new language would require parental notification and consent prior to the collection of persistent identifiers where they are used for purposes such as amassing data on a child's online activities or behaviorally targeting advertising to the child. Therefore,

¹⁵ Children's Online Privacy Protection Rule; Proposed Rule, 76 Fed. Reg. 59,804, 59,812 (Sept. 27, 2011) [COPPA NPRM].

¹⁶ CSM White Paper, *supra* note 3, at 2.

¹⁷ *Id.* at 3.

¹⁸ *Id.* at 4.

¹⁹ COPPA NPRM, *supra* note 15, at 59,812.

operators such as network advertisers may not claim the collection of persistent identifiers as a technical function under the “support for internal operations” exemption.²⁰

The definitions should not permit tracking by commonly owned online services. An entity may have common ownership, affiliate, or other control relationship with several websites or online services. The Commission should clarify that linking across these commonly owned online services is covered by paragraph (h) and requires clear parental consent. Further, the Commission should clarify that common ownership, control, or other relationships between online services do not permit information sharing as an “internal operation.” This is an important concern.

While it is increasingly common for several different brands to exist under a common corporate umbrella, those brands are still seen by most consumers as different identities. For example, PepsiCo owns the Gatorade, Frito-Lay, and Pepsi Cola brands.²¹ Some brands have further sub-brands, such as Frito-Lay, which markets the Fritos, Cheetos, Tostitos, and Doritos brands.²² Consumers see them as individual brands. Thus, information linking between www.doritos.com and www.mountaindew.com should not be considered for the purposes of internal operations – despite the common ownership – and should be captured by the definition “links the activities of a child across different websites or online services.”

Similarly, a social networking service may allow application providers to offer games and other extensions to users of its social networking service. Further, the social networking service may directly own, have a controlling interest in, or have another relationship with some of these application providers. For the purposes of (h), the social networking service and apps should be

²⁰ *Id.*

²¹ PepsiCo Brands, <http://www.pepsico.com/Brands.html>.

²² Frito Lay, Full List of Brands, <http://www.fritolay.com/our-snacks/full-list-of-brands.html>.

considered “different websites or online services,” regardless of the ownership structure. Likewise, the linking of information between the social networking service and apps should not be considered an “internal operation” of the company that commonly owns or controls the app and the social networking service. The definitions should be guided by what is clear to a consumer, rather than by what is described on a corporate organizational chart. This is a particularly important distinction where children and families are concerned.

IV. UPDATES TO THE COLLECTION OF PERSONAL INFORMATION

The Commission proposes other updates to protect the collection of personal information. Common Sense Media is generally supportive of these updates and comments to improve them.

A. “100% deletion” Should Allow More Reasonable Measures

The Commission proposes to change the “100% deletion” standard. The Commission proposes:

An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child’s postings *before* they are made public [*emphasis added*]²³

The new standard should reflect the continuing obligation under COPPA to not collect children’s personal information without parental consent. Further it should provide more scope to the reasonable measures operators should take to delete personal information. Thus Common Sense Media proposes that the change instead be:

An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child’s postings *that* are made public...[*emphasis added*]

²³ COPPA NPRM, *supra* note 15, at 59,809.

This phrasing should encourage operators to take measures even after publicly posting information. The intent should not be to reduce the responsibilities that an operator has before information is made public, but rather to promote the development of methods to protect children after a posting is made public. Common Sense Media recognizes that today, information that is publicly posted is often difficult to remove from further circulation, so measures before public posting will continue to be key to protecting children's information.

With the proposed changes, however, operators will have greater incentive to respond to user notices and requests. Operators could innovate by implementing tools such as an "eraser button" or other technologies which allow a user to delete information. Further, a reasonable operator should be expected to develop a method for a parent to contact them and ask that information be redacted and should respond immediately to such requests. The Commission's proposed phrasing, with the term "before," might be interpreted to mean that their responsibility ends with the public posting. We strongly urge instead that the responsibility be ongoing and that it reflect parents' requests for redaction, without reducing the responsibility of operators to remove personal information before publically posting.

B. "Online contact information" & "Screen or user names"

Common Sense Media supports the Commission's proposals to include as personal information screen and user names and the various forms that online contact information can take beyond email addresses. The Commission proposes to change the definition of "Online contact information" to:

an email address or any other substantially similar identifier that permits direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier.²⁴

²⁴ COPPA NPRM, *supra* note 15, at 59,810.

The Commission further proposes:

That screen (or user) names be categorized as personal information when they are used for functions other than, or in addition to, support for the internal operations of the Web site or online service.²⁵

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. Further, various online forums permit users to contact each other via personal message, or “pm.”²⁶ On the Facebook social network, users can “tag” other users in content, causing them to be contacted.²⁷ 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.”²⁸ The service skims data from social networking services and compiles it into profiles.²⁹ 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.

C. Photographs & Videos

Common Sense Media strongly supports the inclusion of photographs and videos as part of updating COPPA to keep up with technological developments. Further, we recommend that the

²⁵ *Id.*

²⁶ See, eg, phpBB, Communicate with Privacy Messages, http://www.phpbb.com/support/documentation/3.0/userguide/user_pm.php.

²⁷ Tom Ochino, *Tag Friends in Your Status and Post*, The Facebook Blog, Sept. 10, 2009, <https://www.facebook.com/blog.php?post=109765592130>.

²⁸ Spokeo Username Search, <http://www.spokeo.com/username-search/>.

²⁹ Cyrus Nemati, *SpokeNo*, Center for Democracy and Technology, July 1, 2010, <https://www.cdt.org/blogs/cyrus-nemati/spokeno>.

Commission include in its definition of personal information the collection of “any biometric identifier.”

When COPPA was proposed, Congress and the Commission were concerned with websites that collected and shared children’s personal information online without parental consent. Sen. Bryan stated:

I was, frankly, surprised to learn the kinds of information these websites are collecting from our children. Some were asking where the child went to school, what sports he or she liked, what siblings they had, their pet’s name, what kind of time they had after school alone without the supervision of parents.³⁰

Now the personal information being posted online includes images, audio, and videos. This important update is clearly in keeping with the original goals of COPPA.

The definition should also include other biometric identifiers. The Commission correctly notes the rise of facial recognition as a concern to spur coverage of images. However, facial recognition algorithms often process data that may not fit under the definition of “a child’s image.” For example, facial recognition can use landmarks such as the relative distance between points on a face.³¹ Further, NIST has pointed to the potential for touchscreen mobile devices to generate mobile fingerprint IDs.³² Thus, the COPPA rule should cover any biometric identifier, not just “image” or “voice.”

D. Geolocation & GPS Data

Common Sense Media strongly supports the Commission’s proposal to include geolocation information under the definition of information protected by COPPA. This decision clearly updates the rule to reflect the current electronic and digital world. The Commission proposes to

³⁰ 144 Cong. Rec. S8482 (July 17, 1998) (Statement of Sen. Bryan).

³¹ See, eg, J. Shi a , A. Samal, D. Marx, *How effective are landmarks and their geometry for face recognition?*, 102 COMPUTER VISION AND IMAGE UNDERSTANDING 117 (2006). See also Federal Trade Commission, *Face Facts: A Forum on Facial Recognition Technology*, Dec 8, 2011 [remarks of Ralph Gross and Dr. P. Jonathon Phillips].

³² NIST, *Handheld Touch Screen Device May Lead to Mobile Fingerprint ID*, Dec 15, 2009, http://www.nist.gov/itl/iad/fingerprints_121509.cfm.

include within the definition of personal information “geolocation information sufficient to identify street name and name of a city or town.”³³ Common Sense Media understands the sufficiency to describe the type of geolocation information, not a particular data point. If a particular coordinate is not near a town or a street but is of a type and of such accuracy that in a different location it would be near a town or a street, then that coordinate would still be covered. Indeed the Commission comments that “geolocation data that provides information at least equivalent to ‘physical address’ should be covered as personal information.”³⁴

Online services and operators no longer collect just traditional street addresses; they also gather Global Positioning System data and other indicators of location that can be just as accurate, if not more so. Even more important, while users may actually enter their street address information into a service, geolocation information may be collected by a service with little or no user knowledge.

For kids and families, this is absolutely critical: Knowing what a child or teen does online at home is one thing. Knowing where they go after school, with whom they visit, and what they search for is not only incredibly invasive, it is potentially dangerous and a fundamental violation of their personal privacy and self-interest. Mobile companies and app developers that have a cavalier attitude about this topic need a very clear wake-up call. Common Sense believes all users should have “opt-in” protections for location information for all mobile services and apps, and it is especially important to have “opt-in” protections for children and teens. Location privacy isn’t merely a concern for parents of younger children, but also for teens. The Common Sense/Zogby poll found that 81% of teens say search engines and social networking sites should

³³ COPPA NPRM, *supra* note 15, at 59,830.

³⁴ COPPA NPRM, *supra* note 15, at 59,813.

not share their physical location with other companies without their specific authorization.³⁵

Strengthening COPPA as well as exploring this issue more broadly for teens are clearly in order.

V. IMPROVEMENTS TO NOTICE SHOULD BE CLEAR TO PARENTS, PUBLIC

Common Sense Media has consistently called for major and credible improvements to notice practices³⁶ and supports the Commission's proposed changes to the notice under COPPA.

Parents want clear privacy policies. In the Common Sense/Zogby poll, 91% of parents (and 81% of teens) said that they would take more time to read terms and conditions if they were shorter and written in clear language. There is room for improvement of notices, given the general belief that few users – children or adults – read online privacy policies and terms of service.

Parents and children – and companies themselves – would be far better served if sites and services also provided clear and understandable summaries of their privacy policies, with links to longer legal documents for users who want more information. In a time when one of the most popular social networks uses messages no longer than 140 characters, it is hard to believe that sites cannot clearly summarize their privacy policies in a short paragraph. This is what consumers need, especially kids and families.

The Commission proposes to require the listing of all operators of an online service and to provide a sample of what data is collected, how it is used, and the operator's disclosure practices.³⁷ The Commission's proposed changes will help more parents understand how and why their children's personal information is being used and help parents get more involved in what their children are doing online. Equally as important, Common Sense hopes more sites and

³⁵ CSM White Paper, *supra* note 3, at 3.

³⁶ *Id.* at 4.

³⁷ COPPA NPRM, *supra* note 15, at 59,815.

services will use privacy notices as an opportunity to educate parents – and all users – about their privacy practices and about smart ways to protect personal information. The recent Microsoft study found that many parents do not understand why they see age-restriction messages on sites.³⁸ Improving those messages and providing links to clear and simple explanations about why the site chooses to restrict by age and about the site’s general privacy practices, would provide an important public service and would also be smart business practice.

VI. PROPOSED DATA SECURITY UPDATES

Common Sense Media supports the proposed data security, retention, and deletion updates.

The Commission proposes to add a rule requiring operators to ensure that third parties are taking adequate security measures:

The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The operator must take reasonable measures to ensure that any service provider or any third party to whom it releases children’s personal information has in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information.³⁹

Further, the Commission proposes to add a new retention and secure deletion requirement:

An operator of a website or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. The operator must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.⁴⁰

Third parties should be held to the same security standards as operators, and operators are in the best position to ensure this. The Commission’s proposal achieves this. Further, the retention limits and requirement for secure deletion should help prevent security breaches by limiting the

³⁸ boyd et al., *supra* note 9.

³⁹ COPPA NPRM, *supra* note 15, at 59,821-22.

⁴⁰ *Id.* at 59,822.

amount of data that is stored and ensuring that it is disposed of properly. Protecting children's information from breaches is not simply a matter of safety, it is a matter of security with potential lifelong impact.

A recent Commission workshop highlighted the growing dangers of children's identity theft,⁴¹ and a report from Carnegie Mellon University identified some of the related risks:

A child's identity is a blank slate, and the probability of discovery is low, as the child will not be using it for a long period of time.

The potential impact on the child's future is profound; it could destroy or damage a child's ability to win approval on student loans, acquire a mobile phone, obtain a job, or secure a place to live.⁴²

The report also identified that children had an attack rate that was 51 times that of adults.⁴³

Following the event, the Commission issued an alert to parents on how to protect their children's data at school.⁴⁴

The Commission's security, deletion, and retention updates to the COPPA rule are in line with the protection that children's data deserves.

VII. ENCOURAGING MORE PARENTAL CONSENT MECHANISMS

Common Sense Media supports the Commission's proposals to encourage new parental consent mechanisms. We propose a change to increase the proliferation of Safe Harbor-approved consent mechanisms. As Microsoft's research on parental attitudes regarding Facebook and other

⁴¹ Federal Trade Commission, *Stolen Futures: A Forum on Child Identity Theft*. July 12, 2011, <http://www.ftc.gov/bcp/workshops/stolenfutures/>.

⁴² Richard Power, *Child Identity Theft: New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers*, 3 (2011), <http://www.cylab.cmu.edu/files/pdfs/reports/2011/child-identity-theft.pdf>.

⁴³ *Id.* at 9.

⁴⁴ Federal Trade Commission, *FTC Consumer Alert: Protecting Your Child's Personal Information at School*, (Sept. 2011), <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt056.shtm>.

surveys show, parents want to be involved. Parents are helping their kids create accounts.⁴⁵ Overwhelming numbers (93%) say that they should have the final say about whether their children can use online services (in contrast to the company, the government, or the child).⁴⁶

A. Race to the Bottom Problem in Safe Harbor Approval of New Parental Consent Mechanisms

The Commission proposes to allow Safe Harbor providers to approve new parental consent mechanisms. Further, the Commission requires periodic reports of these new mechanisms one year after the rule takes effect and every 18 months thereafter. Common Sense Media is deeply concerned that Safe Harbor providers will have an incentive to deliver to operators more users with verified parental consent at a lower cost to the providers – and that this incentive may lead to a “race to the bottom,” where Safe Harbor providers compete to offer lower and lower standards of verified parental consent.

To address this problem, the Commission should require that approvals of new parental consent mechanisms by Safe Harbors be publicly disclosed, including by report to the Commission, within 30 days of their use. This will reduce the competitive benefit of lowered consent standards. Faster disclosure will further the proliferation of new consent mechanisms.

B. Eliminating Email Plus

Common Sense supports the FTC’s proposal to eliminate email plus. From the earliest discussions about the COPPA rule, it was widely recognized that email with a follow-up contact to the parent is not a highly reliable way of verifying that an actual parent is the one giving consent.⁴⁷ This is why the sliding scale was established, limiting the email plus approach to

⁴⁵ boyd et al. *supra* note 9, at 9.

⁴⁶ *Id.* at 13.

⁴⁷ COPPA NPRM, *supra* note 15, at 59,819.

companies that keep children’s information internal. It is also why the Commission originally set the sliding scale approach to expire two years later. Since then, there have been several extensions of the sliding scale approach but little progress in technology that would make parent verification more reliable at a reasonable cost.

Common Sense Media sees this proposal as a wake-up call to industry leaders: In this particular case, as in many areas, we have seen many companies innovate to collect information and far too few companies innovate to protect information. That paradigm must change, and the Commission must continue to push for innovations that protect kids and families.

VIII. THE COMMISSION SHOULD RECOMMEND PROTECTIONS FOR ADOLESCENTS

The Commission states that it “continues to believe that the statutory definition of a child remains appropriate.”⁴⁸ However, the Commission goes on to detail the particular privacy challenges faced by teens, such as their impulsiveness, their vulnerability to identity theft, and the adverse effects on their educational and employment opportunities.⁴⁹ After acknowledging the particular privacy concerns of teens, the Commission notes that it is “exploring new privacy approaches that will ensure that teens – and adults – benefit from stronger privacy protections.”⁵⁰ While the proposed COPPA updates will be an important step for younger children, it is patently clear that adolescents also need privacy protection. Indeed, new legislation has been introduced that provides a strong baseline and addresses an important gap in industry self-regulatory efforts. This remains a huge concern for American parents, educators, and young people.

⁴⁸ *Id.* at 59.805.

⁴⁹ *Id.*

⁵⁰ *Id.*

H.R. 1895, “The Do Not Track Kids Act” foresaw many of the changes that FTC proposed in its COPPA NPRM, and it also provides important new protections for adolescents. Teens would receive explicit protections from behavioral marketing.⁵¹ Further, operators of teen websites would have to provide a Digital Marketing Bill of Rights for Teens.⁵² These rights would be modeled on principles of Fair Information Practices. The FTC could have rulemaking power over these rights. Teens’ geolocation information is protected under H.R. 1895, and they are included under the proposal for an “eraser button.”⁵³ These protections would empower teens themselves, without using the COPPA model of verified parental consent for teens.

H.R. 1895 also picks up where current industry self-regulatory efforts fail to protect youth. The current Self-Regulatory Program for Online Behavioral Advertising offers no protections for adolescents and offers children under 13 the mere promise that participants will follow COPPA.⁵⁴ This is clearly not sufficient protection where the basic well-being of America’s children and youth is concerned and at a time when extraordinarily rapid technological change continues to put their privacy – not to mention their healthy social and emotional development – at risk.

IX. CONCLUSION

The FTC’s COPPA proposal represents a significant step in empowering parents and updating protections for children online. The FTC’s thoughtful and reasoned approach reflects the reality of some present threats to children’s privacy in a 24/7 digital world. Most importantly, the revisions build on the fundamental purpose of COPPA: empowering parents and guardians.

⁵¹ Do Not Track Kids Act of 2011, H.R. 1895, 112 Cong. §4.

⁵² *Id.* at §5.

⁵³ *Id.* at §6, § 7.

⁵⁴ The Self-Regulatory Program for Online Behavioral Advertising, <http://www.aboutads.info/>.

While the FTC revisions will keep COPPA's protections for children under 13 up to date, there are still critically important online privacy concerns for adolescents ages 13 and older. We look forward to further action from the Commission to recommend far-reaching protections for adolescents that address their particular vulnerability to predatory techniques and that give them the tools and protections they need to thrive and mature in this new digital world.

Respectfully submitted,

Guilherme Roschke
Policy Counsel
Common Sense Media

Dec. 22, 2011