Reply Comments

of
The Association for Competitive Technology

on
COPPA Rule Review, 16 C.F.R. Part 312, Project No. P104503

September 24, 2012

The Association for Competitive Technology (ACT) thanks the Federal Trade Commission (FTC or Commission) for the opportunity to submit this reply to the Commission's August 2012 Supplemental Notice of Proposed Rulemaking (S-NPRM) to the Children's Online Privacy Protection Rule (COPPA).[1]

ACT is an international advocacy and education organization for people who write software programs--referred to as application developers--and providers of information technology (IT) services. ACT represents over 5,000 small and mid-size IT firms throughout the world and advocates for public policies that help our members leverage their intellectual assets to raise capital, create jobs, and innovate.

Our goal is to help explain how small businesses that are fueling explosive growth in the mobile apps marketplace have become aware of their responsibilities under COPPA, how the rule changes outlined in the FTC's S-NPRM may affect them, and how small businesses are attempting to meet the goals of COPPA through innovation and parental outreach.

We repeatedly speak in public forums on the issue of protecting children with respect to technology and, more specifically, apps. We testified on the issue of child protection at the House Energy and Commerce Committee's hearing on "Protecting Children's Privacy in an Electronic World."[2] We hosted a panel with Director Mary Engle and the Family Online Safety Institute addressing this new set of proposals. And most recently ACT authored one of the most comprehensive studies of the businesses creating the app economy titled "Apps Across America."[3]

Beyond our policy work, many of our members are part of Parents With Apps, an online community of family-friendly developers, who have a direct interest in the outcome of the COPPA NPRM.

As we noted in our December 2011 filing on the original NPRM, app developers are concerned that, in an effort to modernize COPPA, the FTC is poised to create regulatory burdens that will stifle innovation, hurt job creation, and paradoxically force developers to collect more information on children in order to "protect" them.

While we appreciate the FTC's efforts in the new S-NPRM to understand the ecosystem and take into account the way that mobile applications work, we are concerned that this new proposal fails to take into consideration some of the points raised in our previous filing, and creates a new set of problems of even greater consequence.

Finally, we believe the Commission must look to regulations that are not strictly for the purpose of restraint, but ones that create solutions to acquiring verifiable parental consent, including improvement of existing services and support multi-operator systems.

We see three major problems with the rule which could at best undermine the FTC's efforts, and at worst, utterly destroy educational apps for children:

1. **The S-NPRM underestimates the impact of affected parties by more than 5660% and will conservatively cost educational app developers $250 million in legal fees.**

2. **The S-NPRM attempts to capture the spirit of the new interconnected app economy by altering the definition of "operator" and adding a new "reason to know" standard; however this change could result in the complete removal of all child directed apps from stores/websites which "curate" and from tools that help developers improve applications.**

3. **The S-NPRM attempts to deal with data collected for internal uses only, but its overly proscriptive approach creates significant problems for what is obviously legal and beneficial conduct.**

Beyond these truly "no-go" problems, the S-NPRM has not yet sufficiently addressed questions regarding screen names, persistent identifiers, and applications directed at parents which contain content appropriate for kids. We urge FTC to reconsider this S-NPRM in light of the current ecosystem and the damage that could be done by a well-meaning but misguided rule.

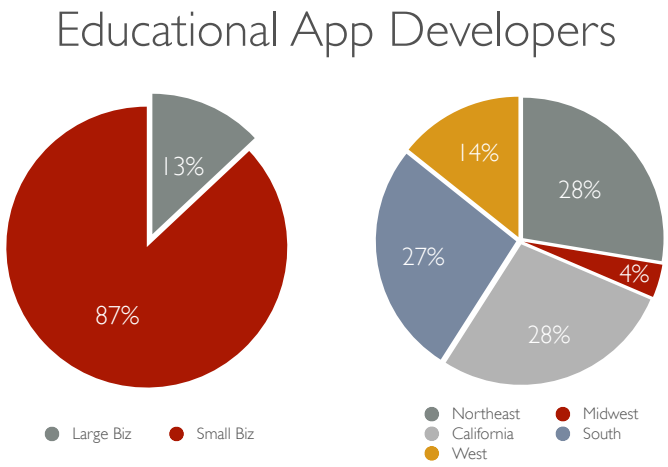
---

[1] Fed. Reg. 59804, Vol. 76 No. 187 (Sept. 27, 2011).
[2] U.S. House Energy & Commerce Committee, Hearing, Protecting Children's Privacy in an Electronic World (Oct. 5, 2011).
[3] "Apps Across America," Association for Competitive Technology (July 18, 2012), *available at* http://actonline.org/files/Apps-Across-America.pdf.

ACT July 2012 Study: Small Business Dominates the Educational App Marketplace

In order to provide the FTC with relevant industry data, ACT recently completed a new analysis of the current mobile app ecosystem, examining apps not only by revenue, but also by type. We looked at the top 800 apps across the productivity, education, business, and entertainment categories. For the purpose of this S-NPRM, we will focus on just one category: Education. Our analysis[4] used publicly available data; as Apple and Android represent 75% of the smart device market, we focused our analysis on those two app stores. As of September 2012, there were more than 74,000 education apps in the iTunes store, and 30,000 in the Android store.[5]

According to our findings, educational app makers represent one of the most diverse populations in the ecosystem. Dominated by small businesses, this group is particularly vulnerable to regulation that imposes significant start-up fees and legal costs.



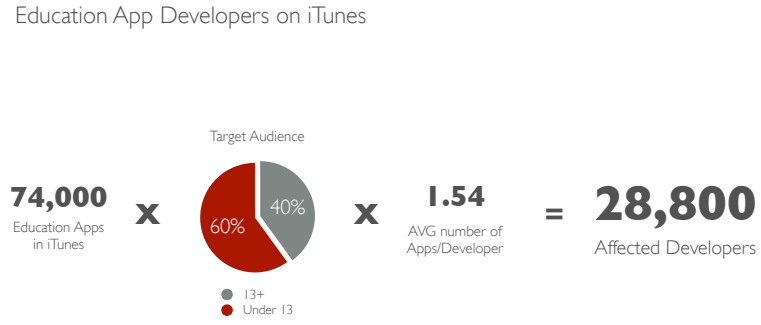
Our research found that 87% of educational apps are created by companies qualifying as "small" by SBA guidelines. And further analysis revealed that nearly all of that 87% was comprised of companies with fewer than 10 full time employees.

This educational app sector is also home to tremendous regional diversity. 29% are produced in California based, with the South accounting for 28% and the Northeast 24%.

Beyond regional diversity, educational apps also showed a higher percentage of different developers on the top applications. Unlike the game sector, where one large developer may have several applications in the top 100, Educational Apps tended to be much closer to a one-to-one ratio between app and creator at 1.54 apps per developer.

Why the FTC's estimate of affected entities is colossally wrong

The FTC has estimated 500 existing education app makers will be affected by the proposed rule, and an additional 125 newly affected entities each successive year.[6] While some may object to our strong wording to describe the FTC's estimate of affected entities, we were unable to find a gentler way to account for the vast difference between the FTC's figures and readily available facts.



As noted, over 74,000 education apps are available in the iTunes app store. Our research revealed that education app makers are more likely to develop one or two apps, rather than a whole series of work-alike applications. We found a 1.54 ratio of education app-to-app creator with more than 60% of apps in this marketplace directed at children under 13.

---

[4] To explore the changes taking place, we surveyed the top 800 apps in the Apple and Android App Stores across the categories of productivity, education, business, and entertainment. We then analyzed each app by revenue, business model, and the location and size of the company developing it to better understand who is behind the explosive growth of the app economy.

[5] "App Store Metrics," 148Apps.biz (accessed September 21, 2012), *available at* http://148apps.biz/app-store-metrics/; "Android Statistic Top Categories," AppBrain (accessed September 21, 2012), *available at* http://www.appbrain.com/stats/android-market-app-categories.

[6] ACT serves as policy support for Moms with Apps / Parents with Apps (MWA), a collective of educational app developers who provide technical and business support for each other. As of September 1, 2012 there were more than 1,200 members of MWA – each one very possibly an affected entity. That number alone contradicts the FTC's estimates.

Looking only at this limited subset of the iTunes app store, the number of developers potentially affected by this rule would exceed 28,800 – a number 250 times greater than the FTC's estimate for the entire industry.

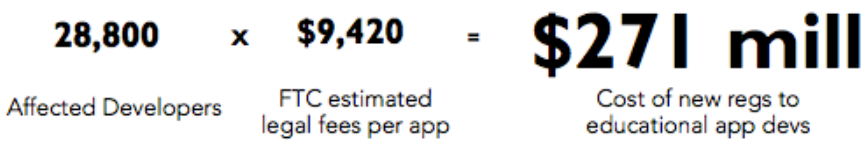
Cost of Compliance and "Reason to Know" Will Hurt Educational Apps the Most

The distinction between existing and new business is a specious one. The reality is that COPPA compliance may very well cost an existing business more than a new one, but at the very least, it will cost as much[7].

The Commission has estimated the costs of compliance for new entities as:

> *Thus, for the estimated 125 additional new operators per year, 7,500 cumulative disclosure hours would be composed of 6,250 hours of legal assistance and 1,250 hours of technical support. Applied to hourly rates of $180 and respectively. $42, respectively, associated labor costs for the 125 additional new operators potentially subject to the proposed amendments would be $1,177,500.*

That's $9,420 per developer. The total cost of this new regulation to education app developers on the iTunes store alone would be more than a quarter billion dollars. These massive costs would completely change the face of the ecosystem, marking the end of free apps and putting these valuable education resources outside the reach of middle class families. For small business app companies whose innovative learning tools are revolutionizing early education, their hope of creating low cost apps and steadily growing their business has evaporated.



According to recent analysis by Distimo and research by Flurry, the average total earnings on Android are only $5,350 per app. On the Apple, Microsoft and Blackberry platforms, average earnings are higher, but do not exceed much more than $10,000 per app per year.

Separating out educational applications from the broader ecosystem, the average dollars earned per app gets even smaller. The educational app space is populated by not just small, but tiny companies, often motivated by the desire to improve educational opportunities for their children. In some cases, like Cheryl Bregman's application to help children with autism communicate with others, the "market" size of the application may be less than $10,000. At ~$10,000 she is unlikely to ever recoup her costs of COPPA compliance, much less pay the developers, artists and dictionary creators who worked to build the app.

Although the FTC may contend not all apps would need to pay the ~$10,000 in legal fees, we would argue that the S-NPRM's creation of a "reason to know" standard will force smart device platforms to require all applications directed at children to provide verifiable parental consent in order to avoid liability, regardless of information collected.

The Commission proposes that third parties should be independently responsible under COPPA if they "know or have reason to know" they are collecting "personal information" from a site or service that is directed to children. According to the commentary provided by the Commission, a party would have a "reason to know" that the site or service is directed at children if "credible information" is "brought to their attention[.]"[8] The "reason to know" standard is not accompanied by any guidance as to who would provide credible information or how it could be brought to a party's attention.

These changes would fundamentally alter the impact of COPPA on third parties, including platforms, plug-in creators, and analytics providers. The S-NPRM would create new COPPA liability where there is the potential to have "reason to know," in spite of the fact that third parties may have no idea if any COPPA relevant information

---

[7] "It is always much more expensive to bolt-on privacy to a product once it has left the production line than to build it in from the start" *Privacy built-in rather than bolted-on – a mere vision or first use cases? Dr. Alexander Dix, LL.M. Berlin Commissioner for Data Protection and Freedom of Information , 10th Privacy Enhancing Technologies Symposium 23 July 2010 Berlin, Germany*

[8] S-NPRM at 46645.

being collected. Therefore prudent legal counsel would suggest that all applications directed at children be treated as collectors of information. Ironically, third parties who provide essential curated services for app developers, making their platforms more trustworthy for consumers, would be more likely to face this problem for apps that it reviewed, or "curated," before being placed for sale in the digital store -- third parties that do nothing to protect consumers would be off the hook. The act of reviewing an app for compliance with the third party's terms of service could be seen to give the third party "reason to know" the app is directed at children.

This fundamental change to COPPA would force third parties to take severe steps to prevent liability exposure. Third parties like mobile app platforms would find themselves in the position of being liable under COPPA for the actions of apps on their platforms. In order to ensure they are not subject to liability based on the actions of the operator, third parties will have to demand developers provide assurances that their apps comply with COPPA. This means that all educational apps would have to spend ~$10,000 in legal fees to provide third parties that all app developers use, like mobile app platforms such as iTunes and Amazon, with the required assurance of COPPA compliance. Unlike games or other apps, educational apps cannot simply age-gate to limit use. These are products intended for use by children, and by their very nature must be explicit in the age-range served; math games for 7 year olds are different than those for 14 year olds.

Imagine the mother or father who realizes that their child would really benefit from a new way to learn about dinosaurs using Microsoft Surface technology. How do you think they will react when they discover that their first outlay of capital is not to an artist, or a programmer, but to a law firm, possibly before a single line of code is written? In our private polling of top educational app developers, there was nearly unanimous agreement that an upfront ~$10,000 fee would have dissuaded them from ever writing their app.

Further consideration should be given to the confusion this would create among third parties which already follow the practice of "age-gating" to ensure that they do not collect information on children. For example, plug-ins like Twitter are commonly used by operators to add functionality to their site or service. In order to have a Twitter account, Twitter "age-gates", requiring a user to verify that they are 13 or older. This "age-gating" theoretically gives Twitter *actual knowledge* that they are not gathering information prohibited by COPPA. However, if such plug-in is used on a site directed at children under 13, would the presence of that user on that site somehow diminish or negate that actual knowledge? Saying that Twitter could be liable for collecting data about a person that it has "actual knowledge" is over 13, where Twitter is operating a general audience service, is essentially saying that Twitter is held to a higher standard as a plug-in operator than the website operator itself. Certainly this can't be the intended outcome.

Expansion of the Term "Operator" Would Restrict Crucial Innovation

The Commission has proposed to extend operator liability under COPPA to include the data collected by third parties if personal information is collected "in the interest of, as a representative of, or for the benefit of" the operator. This goes far beyond what the Commission has consistently viewed as the nature of an operation; that is the ownership or control of data. As stated in the FTC's 1999 Statement of Purpose for COPPA, an site or service is not an operator where it "merely acts as the conduit through which the personal information collected flows to another person or to another's Web site or online service[.]"[9] However, under the S-NPRM an app developer would now be liable for the practices of a third party where the developer has neither control over the data nor how it is used. Where there is no ability to give "notice and obtain consent from parents" for the purpose of COPPA compliance because the developer does not "own, control, or have access" to the personal information collected or prevent future use of the data, liability should not be imposed.

Operators under COPPA are liable for the acts of a third party where data is collected to their benefit. The S-NPRM redefines benefit to mean any advantage that might result from a relationship between the operator and the third party. However, while revenue may pass between the third party and developers, the "benefit" has always been read as control of the data. The S-NPRM would impose liability risks on developers who are not in a position to control compliance by third parties.

The Commission cites "changes in technology" as the reason to read COPPA's definition of an "operator" as a person "on whose benefit" personal information is collected and maintained far beyond the way it has traditionally

[9] Federal Trade Commission, 1999 Statement of Basis and Purpose to the COPPA Rule, 64 Fed. Reg. 59888, 59891 (Nov. 3, 1999).

been interpreted.[10] However, small businesses like app developers have always relied on third parties for services that they don't have the resources to perform in-house. To stretch that meaning such that developers are liable for the actions of third parties they have no control over is to overly-burden numerous small businesses.

Take, for example, *XYZ magazine* has created an app is directed to girls ages 12 to 15. The app created by *XYZ* does not collect any information from users. However, *XYZ* has placed a Google+ plug-in within the app that allows users to Google Talk with their friends without leaving the app. While this plug-in adds important functionality to the app, *XYZ* app does not collect any information or have access to information collected from its plug-ins. If the S-NPRM is adopted, *XYZ* would now be liable for the data collection by Google+, which they did not encourage the child to provide[11] and have no control over.

The result is app developers would limit their use of any third parties to ensure they are not held liable for the actions of those over which they have no control. They would no longer use third parties like plug-ins to help add functionality to their apps or analytics companies which help them identify the strengths and weaknesses of their apps. Without these important tools to manage, improve, and monetize their apps, innovation in the educational app industry would be choked. Even worse, potential liability could drive potential developers away from educational apps all together.

The S-NPRM attempts to deal with data collected for internal uses only, but creates too high a barrier by prohibiting use of that data "for any other purpose"

A review of the September 2011 and August 2012 NPRMs show that the FTC is working to understand and improve the ability of developers to use third party tools for internal operations:

> *Support for the internal operations of the website or online service means those activities necessary to: (a) maintain or analyze the functioning of the website or online service; (b) perform network communications; (c) authenticate users of, or personalize the content on, the website or online service; (d) serve contextual advertising on the website or online service; (e)* ~~*maintain the technical functioning of the website or online service, to*~~ *protect the security or integrity of the user, website, or online service;, or (f) to fulfill a request of a child as permitted by §§ 312.5(c)(3) and (4),; so long as* ~~*and*~~ *the information collected for such* ~~*purposes*~~ *the activities listed in (a)--(f) is not used or disclosed to contact a specific individual or for any other purpose.*

Clearly the Commission is to trying to find a way to satisfy all parties. Unfortunately, the addition of "for any other purpose" makes the uses itemized in (a)-(f) overly proscriptive. One of the most obvious limitations that will flow from this narrow list of uses is benchmarking. From our extensive discussions with FTC staff, we know the Commission understands the value of analytics to improving applications and identifying new opportunities. Unfortunately, the "for any other purpose" restriction would prevent the companies who build analytics tools from analyzing, benchmarking and improving the very products that are so helpful to developers.

The FTC correctly identifies security under (e) as a potential permitted use under this provision; third party tool creators could be collecting information to help with security, but because they are not the support for internal operations of the first party, the use of data could put them at risk.

We recommend the FTC either expand the activities permitted to include greater third party usage, or remove "for any other purpose".

Personal Information and Persistent Identifiers

ACT continues to stress that the FTC's to include unique or persistent identifiers, as personal information is problematic and likely a violation of Congressional intent.

---

[10] S-NPRM at 46644.

[11] The FTC has suggested that having a social networking button or plug-in on an app or website should not rise to the level of encouraging children to provide information -- the mere existence of a chat plug-in does not rise to the level of collecting information.

Congress considered and dismissed including unique identifiers in the definition of personal information under the original COPPA legislation. This was not merely a Congressional slip; IP addresses and persistent identifiers existed well before the creation of COPPA legislation, and legislators discussed including such language in the bill. Additionally, privacy concerns regarding persistent identifiers were raised in the 1998 FTC Report to Congress on which much of COPPA's language is based.

Therefore Congressional intent was clear when they chose not to include persistent identifiers in COPPA. This conclusion is further bolstered by Congress's enumeration of personal information criteria and specifically omitting persistent identifiers or IP addresses from that list.

Since the drafters of the COPPA legislation did not intend for IP addresses and other persistent identifiers to be personal information, the FTC should not make such a change at this point.

While the S-NPRM attempts to help with the screen name problem, our developers still see problems where the screen name is used to share in-app information or actions, but does not reveal the actual name or contact information of the child. This inability to use screen names hinders multi-user or collaborative learning tools.

Apps for Parents May Have Content Directed at Children

The FTC's attempts to answer the "family friendly" conundrum are laudable, but we seek to clarify that the FTC does not consider apps or websites where the parent is audience, but the content is kid focused an automatic "operator" under COPPA.

For example, a toy store website or app would contain content (pictures and descriptions of toys) which are "likely to attract and audience that includes a disproportionately large percentage of children." Like physical toy catalogs, the content of a toy store website or app will appeal to children, but the operator does not collect data from children, rather from the adults who make the purchases. Kids might bookmark webpage like they once dog-eared toy catalogs before the holidays, but the website is still directed at adults. In order to ensure that websites targeted to adults that contain content which appeal to children, the language of COPPA should clarify that such websites do not fall under its regulations.

New Technologies Can Bring New Forms of Parental Consent, Just Not All at Once

Parental engagement is necessary for truly effective COPPA compliance, therefore we wanted to re-state our previous concerns about killing off email plus, but also offer support for newly suggested ways to achieve multi-operator permission.

We all want parents to know what their child shares online and we want them to be involved; studies show parents are involved in granting consent to their child's use of and sharing on apps, and these parents are engaged in ways that were not true in the PC based website world. Given this heightened awareness by parents, we do not think that removal of easy to understand systems like email plus is likely to create new methods of parental consent. Instead, we need to find ways to make parental consent simpler. Moreover, a recent study found that of the parents are active participants in helping "tween" children sign-up for services that are age gated or require verifiable parental consent. The study went on to state:

> *"Rather than providing parents with additional mechanisms to engage with sites honestly and negotiate the proper bounds of data collection about their children, parents are often actively helping their children deceive the sites in order to achieve access to the opportunities they desire. Were parents and their children able to gain access honestly, the site providers might well present them with child-appropriate experiences and information designed to enhance safety, provide for better privacy protections, and encourage parent-child discussions of online safety. With deception being the only means of access, these possibilities for discussion, collaboration, and learning are hindered."*

Clearly there is a disconnect between the consent of parents and their ability to grant that consent in a COPPA compliant way. So we believe the FTC should re-examine the elimination of email plus to determine if there are other ways to encourage innovation, including investigating alternative systems that are part of social network sites, game systems, and global marketplaces.

COPPA compliance is a substantial hurdle faced by small mobile app developers – who are challenged by screen

size, business size, and evolving business models, but we are innovating and by innovating we can continue to develop educational tools to help children.

Presently, the FTC allows credit card transactions to constitute parental consent. However, these transactions must be for a fee paid though a credit card, and require the parent be notified in advance regarding the type of information collected.

The problem for app developers is that the regulations remain unclear as to whether financial transactions connected to a credit card authorized user account may fall within the existing form of parental consent. For example, when purchasing an app through the iTunes App Store, rarely is a credit card entered. However, to make any acquisition of an app, even a free app, the owner of the iTunes account's password is required. This is akin to entering a banking account number or a credit card number.

The FTC should clarify that the purchase of an app using the password of an account tied to a credit card may be treated the same as if the credit card number itself were entered. Moreover, with most every app purchase, even for no fee, an email confirmation of the transaction is created and sent to the account holder. This allows parents to know what apps have been purchased and installed instantly rather than waiting for the monthly credit card bill. And since this receipt is created and the process is identical whether purchasing for a fee or free, the purchasing of free apps and free in-app purchases could constitute parental consent where the developer first provides notice. Simply put, the combination of clear notification plus the use of a username and password that is a credit card equivalent should be seen as verified parental consent.

Enable platform providers to obtain Parental Consent on behalf of App Developers

A number of practical COPPA compliance challenges arise from the fact that many apps are integrated into and operate through social media and mobile communications platforms that are maintained by a different operator. As a result, certain information, such as the user's IP address, device ID, username or screen name, is sometimes shared between the app developer and the platform provider automatically when a user runs the application. This limited information sharing supports the technical and operational functioning of the app.

One alternative solution is to allow platform providers to offer notice and obtain consent on behalf of the app developer who offers access to online services through the platform. Under this streamlined approach the platform operator would need to notify parents that multiple apps provide online services through the platform, generically describe the types of online services that these apps provide, and explain that these apps may collect and maintain the child's personal information to engage in "support for the internal operations" of the online service.

The platform operator would obtain verifiable parental consent that would cover the collection, use, and disclosure of the child's personal information by the platform provider and app developer, consistent with the disclosures made in the privacy notice. To the extent the app developer would like to use the child's personal information for purposes beyond support for internal operations, the app developer would be responsible for independently providing the parent with notice of these uses and obtaining verifiable parental consent consistent with COPPA.

This approach ensures that parents have meaningful notice of and control over how their children's personal information is collected, used, and disclosed online, without imposing unnecessary burdens and costs on app developers.

ACT understands the FTC has been presented proposals that could help to create a multi-operator environment, and we look forward to working with all parties to make the multi-operator idea a reality.

Conclusion

ACT's members are working hard to change the very nature of our children's lives – through smart device applications that help them learn, explore and communicate. With thousands of parent developers, our members understand most clearly the need to protect children in the mobile and internet environment. There is no stronger group of people with the knowledge and the frontline experience to understand that privacy and innovation are not in conflict. What can create conflict is well-meaning regulation that errs on the side of proscribing innovation in the name of protecting privacy.

The S-NPRM as it stands now fails in its goal to increase security for children while enabling innovation. It scares

vital third parties away from educational app developers, discourages small business participants by requiring exorbitant amounts of time and energy interpreting unclear regulations, eliminates the ability to collect non-personal information to assist in furthering the educational goals of apps, and exposes many new parties to unexpected COPPA liability. We believe that with COPPA, the FTC must take a "first do no harm" approach, and reconsider changes for which there is neither the legislative intent nor the potential risk to children's privacy to require this change. The FTC should focus on creating flexible, simple to implement regulations that protect children, allow parents to monitor and give parental consent, and allow operators and third parties to understand clearly their obligations under COPPA.

We thank the Commission for the opportunity to comment and hope the information we provided helps to further improve and simplify the regulations surrounding COPPA.