

December 23, 2011

VIA ELECTRONIC FILING

Mr. Donald S. Clark
Office of the Secretary
Federal Trade Commission
Room H-135 (Annex E)
600 Pennsylvania Avenue, NW
Washington, DC 20580

RE: COPPA Rule Review, 16 CFR Part 312, Project No. P-104503

Dear Mr. Clark,

Thank you for the opportunity to comment on the Federal Trade Commission's proposed revisions to the Children's Online Privacy Protection Rule. We very much appreciate the opportunity to share our feedback on this important development and look forward to being involved in the continued dialogue.

Introduction and Background

My name is Shai Samet, and I am the founder and president of the kidSAFE® Seal Program. The kidSAFE® Seal Program (also referred to as "KSP" or "we") is a new, emerging safety certification service and seal program designed exclusively for children-friendly websites and applications. Our program is still in a beta trial, although we have several members already participating. We also have a notable advisory board, consisting of renowned Internet safety experts. To learn more about our program, please visit our website at www.kidsafeseal.com.

As the name suggests, our program is focused (first and foremost) on the online safety of children. However, due to the needs of industry, we have also created a membership level that includes the assessment and ongoing oversight of COPPA compliance. It is in this context that we submit to you our comments on the COPPA Review.

Please note that the views expressed herein reflect the views of the kidSAFE® Seal Program, and not necessarily the views of its members. Also, all references to the term "COPPA" are meant to refer to the FTC Rule implementing COPPA (i.e., the COPPA Rule).

General Perspective

Our comment (which starts on page 3) is extremely thorough and covers virtually every aspect of the proposed revisions. Our general perspective can be summarized as follows:

- Although we support many of the proposed changes (with additional modifications and/or clarifications), we take issue with the more drastic changes (e.g., expansion of the definition of personal information, removal of email plus, etc.), as these changes would significantly increase the cost and burden of COPPA compliance and likely result in fewer online activities for kids. As a result, children may seek online activities in places where they don't belong (e.g., Facebook,

YouTube, etc.), posing a greater (not smaller) risk to the safety and privacy of children online. As a new seal program focused on online safety, we do not support such an outcome.

- In a survey conducted by KSP during an industry-wide COPPA webinar¹, a large percentage of companies (61 percent) indicated that COPPA is challenging to comply with in its current form. This suggests we need to find ways to make COPPA compliance easier, not harder.
- We believe significant changes to COPPA will further encourage companies to avoid COPPA compliance entirely (through age screens, fewer interactive activities, etc.), as opposed to encouraging the development of new parental consent techniques or other COPPA solutions.

Format of Comment

The remainder of our comment is organized according to the FTC’s proposal in the Federal Register notice. For ease of understanding, our comments are provided in a simple bullet-list format. For each area, we indicate whether we support or oppose the proposed revision, provide a lengthy description of our comments or concerns, and (in some instances) propose revised wording for the language of the law itself (shown in boxes) or alternative models for FTC consideration. Also, throughout the document, we highlight certain statements for added emphasis or to illustrate our overall position on the topic.

Conclusion

We commend the Federal Trade Commission for its efforts to update COPPA to address new and evolving technologies. As you review our comment, please know that we would be happy to answer any follow-up questions or participate in any advisory group that may be formed to further explore the impact of the proposed revisions.

Sincerely,

A rectangular box with a light blue border, containing a small black arrow pointing to the left, indicating a redacted signature.

Shai Samet, CIPP
Founder & President
kidSAFE® Seal Program

¹ The webinar was conducted on December 15, 2011 and was attended by over 50 industry contacts from a diverse set of both large and small companies, including large and small providers of kid-directed websites, virtual worlds, online social networks, web-enabled game devices, and mobile apps. The results of other polls conducted during this webinar are shared throughout this comment document.

DEFINITION OF CHILD

- **KSP supports keeping this definition (i.e., “12 and under”) unchanged**
- Age-cut off of 13 provides a clear standard for operators to follow and seal programs to enforce
- We have no industry indicators or other data to suggest that the age should be raised/lowered
- In terms of the age lying dilemma², KSP encourages the FTC to explore whether intentional age falsification on the web should be considered a crime, similar to online piracy. In our view, this may be the only effective method of addressing this ongoing and unresolved issue.

ACTUAL KNOWLEDGE STANDARD

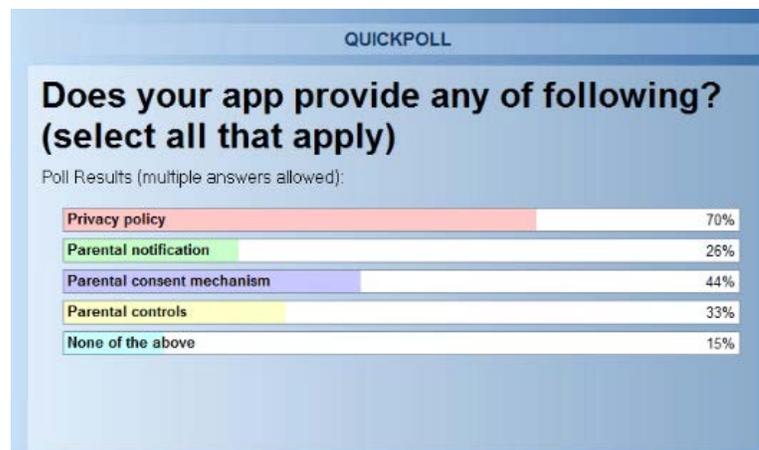
- **KSP supports keeping this standard unchanged** (i.e., sites not directed to children must have *actual knowledge* that they’re collecting personal information from a child under 13 in order for COPPA to apply)
- This standard provides a clear framework for operators to follow and seal programs to enforce
- This standard appears to be the most workable standard for the mobile marketplace, where it is often unknown whether the owner/user of the mobile device is a child
- KSP encourages the FTC to explore whether general-audience social networking sites that are not intended for kids (such as Facebook, Twitter, YouTube, etc.) should be required to have policies that prohibit and police the integration of social networking links or features (such as share functionalities) on kid-targeted websites and mobile apps. To the extent this type of integration continues, these social networks are likely to have actual knowledge of the presence of children on their websites, regardless of the age or date of birth selected during registration.
- For more on issues related to the actual knowledge standard, please see our comments under the section titled [“DEFINITION OF WEBSITE OR ONLINE SERVICE DIRECTED TO CHILDREN”](#)

EVOLVING TECHNOLOGIES (definition of “Internet” and “online services”)

- **KSP is not opposed to the idea of COPPA covering new technologies (i.e., mobile apps, web-enabled gaming devices, etc.); however, actually applying some of COPPA’s requirements to these newer technologies may pose significant practical challenges**
 - For example, two industry surveys conducted by KSP (see [FN1 above](#)) revealed that, despite the growing presence of interactive features within kid-friendly mobile apps, operators of mobile apps are significantly behind with respect to COPPA compliance
 - The more detailed poll results are illustrated at the top of the next page

(continued on next page)

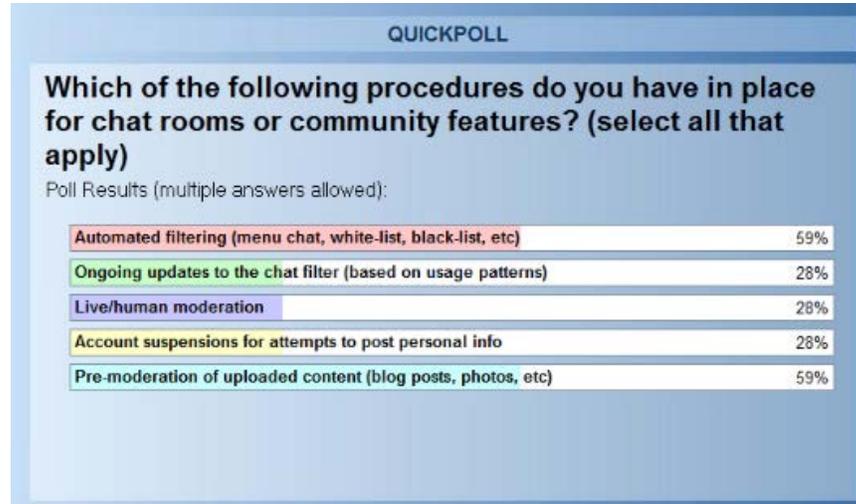
² See study by Dana Boyd, Eszter Hargittai, Jason Schultz, and John Palfrey (Microsoft Research – Nov 2011): [“Why Parents Help Their Children Lie to Facebook: Unintended Consequences of the ‘Children’s Online Privacy Protection Act’”](#).



- Some of the challenges posed by the application of COPPA to the mobile space are discussed in further detail below
 - In general, we encourage the FTC to consider how each of COPPA’s requirements can be eased or simplified in the context of mobile apps
- Another concern we have regarding the expanded understanding of “Internet” and “online services” is the fact that those terms are not consistently applied across the entire COPPA Rule, creating unfairness for mobile app developers. In other words, if the term “online” includes mobile for purposes of COPPA’s scope, then shouldn’t the term “online contact information” also include a “mobile phone number”, which today is the primary method of communication via smartphone devices? Although we recognize that adding a mobile phone number to the definition of “online contact information” may require changes to the underlying COPPA statute, this change is worthy of further consideration, especially given the general unpreparedness of mobile app developers to address COPPA. For example, operators of mobile apps will need to have the luxury of using identifiers that are relevant to its unique ecosystem in order to take advantage of COPPA’s parental consent exceptions (which heavily rely on the use of “online contact information”).

DEFINITION OF “COLLECTS OR COLLECTION”

- KSP supports including under paragraph (a) of this definition that collection also occurs when the child is *merely prompted or encouraged to provide personal information*. This change will clarify that optional data fields on registration forms are equally subject to COPPA requirements, a premise which we have worked with all along
- **In regards to paragraph (b) of this definition, KSP strongly supports the elimination of the “100% deletion standard” in favor of a new “reasonable measures” standard**
 - In our tests to date, we have not found any filtering system to be perfect, and so this change is consistent with the realities and limitations of operating popular community features (such as chat rooms, forums, social networking features, etc.).
 - KSP requests that the FTC provide an illustrative list of procedures that may be considered “reasonable” for purposes of meeting this standard. This list should not be binding or exhaustive; it should simply offer guidance on the topic (similar to what the FTC has offered under the “reasonable security” standard, both inside³ and outside⁴ the context of COPPA). For example, it will be important to know what would be expected of operators at a minimum (e.g., type of chat filter, frequency of live moderation, etc.).
 - In evaluating this area, the FTC may wish to consider the results of an industry survey we conducted on this point (see below). We note that the popularity of some measures over others may be attributed to cost.



- As a seal program focused on the safety of interactive features (and given the expertise of our advisory board), KSP is in a unique position to help the FTC formulate a list of reasonable procedures in this area, and we would be delighted to assist upon request
- We also have specific guidelines already developed in this area

³ See Page 59906 (footnote 284) of the original Statement of Basis and Purpose under the Final Rule (effective April 21, 2000).

⁴ See the various data-security enforcement actions brought by the FTC and other related materials (<http://business.ftc.gov/privacy-and-security/data-security>).

- Note that there’s a great deal of complexity when it comes to keeping interactive and user-generated features free of personal information, profanity, or other inappropriate content. For example, consider whether the “all or virtually all” test would be met if misspellings or abbreviations that hint to personal information could get through a chat filter? **We believe therefore that the FTC is correct in developing a flexible standard which is based on reasonableness.**
- Also refer to the section titled “[SCREEN NAME OR USER NAME](#)” for another important change to paragraph (b) of “collects or collection”
- In regards to paragraph (c) of the definition of “collects or collection”, KSP recommends that the FTC modify the new wording to clarify that “passive tracking” is only considered “collection” when it involves the collection or use of personal information. Although this is indicated in the opening language of the definition, the other two paragraphs (i.e., (a) and (b)) currently restate the reference to personal information, while paragraph (c) does not. Therefore, we recommend amending paragraph (c) as follows:

*“The passive tracking of a child online, **when such tracking involves the collection or use of personal information**”*

- Note that because of the expanded definition of “personal information” (to include “persistent identifiers”), the revision above would still encompass technologies beyond cookies, and address the FTC’s original reason for making the modification

DEFINITION OF “SUPPORT FOR INTERNAL OPERATIONS”

- **KSP supports creating a separate stand-alone definition for this term, although believes that the wording of the definition still needs significant improvement**
- Our concerns and recommendations are as follows:
 - The definition of “support for internal operations” needs to call out more clearly those uses that the FTC has described as being “technical”, but that would not ordinarily be described as technical when explaining them to users. For example, “personalization” and “contextual ads” would not ordinarily be described as technical, although the FTC has stated that it views these uses as “technical” (see page 37 of the proposal) and therefore covered under this definition. The same is true for things like “displaying user names” to other users within a virtual world (see page 30 of the proposal).
 - The definition should also include a reference to protecting the security of “users” (in addition to the security of the site or online service). This is a common form of use, which should be regarded as necessary to the technical functioning of the site/service.
 - It is unclear what is meant by the inclusion of two parental consent exceptions (i.e., Sections 312.5(c)(3) and (4)) under this definition? Also, why are only two out of the six parental consent exceptions included? What about the other four exceptions? Are they not relevant for some reason?

- Based on the concerns above (and other concerns described in sections later), KSP proposes to revise and expand the definition of “support for internal operations” as follows:

- *“Support for internal operations of the website or online service means those activities necessary to (i) maintain **or improve** the technical functioning of the website or online service, (ii) ~~to~~ **provide internal features and activities, including personalization and contextual advertising**, (iii) ~~to~~ protect the security or integrity of the website or online service **or the security of its users**, or (iv) ~~to~~ fulfill a request of a child as permitted by Sections 312.5(c)(1)-(6); and the information collected for such purposes is not used or disclosed for any other purpose.”*
- Alternative definition: *“Support for internal operations of the website or online service means those activities necessary to (i) maintain, **improve, or personalize** the ~~technical~~ functioning of the website or online service, (ii) ~~to~~ protect the security or integrity of the website or online service **or the security of its users**, or (iii) ~~to~~ fulfill a request of a child as permitted by Sections 312.5(c)(1)-(6), and the information collected for such purposes is not used or disclosed for any other purpose.”*

DEFINITION OF “ONLINE CONTACT INFORMATION”

- As already noted above (see last bullet under the section titled [“EVOLVING TECHNOLOGIES”](#)), the FTC should further explore whether “cell phone numbers” can be added to the definition of “online contact information”, without requiring statutory changes. If the scope of the COPPA Rule covers mobile (e.g., mobile apps, web-based text messaging programs, etc.), then we need to find some other common identifier or method of communication closely tied to mobile (such as SMS) that would enable operators to more easily initiate a parental consent process and/or utilize the various parental consent exceptions when dealing with mobile customers.
 - For example, in its current or even modified form, unless a website operator obtained verifiable parental consent, COPPA would not allow an operator to collect a child’s cell phone number via its website for the purpose of sending the child a one-time SMS communication or signing up the child for an ongoing SMS program; however, the collection of an email address for these very same purposes would be allowed. This discrepancy raises concern.

DEFINITION OF “PERSONAL INFORMATION”

SCREEN NAME OR USER NAME

- **KSP does not oppose the addition of screen/user name to the definition of “personal information”, particularly because of the internal operations exemption**
- However, the FTC should provide additional guidance regarding what (if any) uses of screen name would be considered “non-internal” (and thus “personal information”). There were no examples given in the FTC’s proposal.
- Also, the definition of “support for internal operations” should be further modified (as suggested [above](#)) to clarify that internal uses of screen names are not considered “personal information”, even when those uses involve the display of screen names in public areas (e.g.,

chat rooms, community areas, leaderboards, etc.). Although the FTC has indicated that these uses are considered “internal operations”, this conclusion is not obvious from the wording of the definition itself.

- In addition to further modifying the definition of “support for internal operations”, and for the sake of ensuring screen names are not considered “personal information” when used *within* a site or online service, we recommend adding the following language to paragraph (b) of the definition of “collects or collection”:

*“Enabling a child to make personal information publicly available in identifiable form. 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 posting before they are made public and also to delete such information from its records. **An operator shall also not be considered to have collected or disclosed personal information under this paragraph if it collects and publicly displays a child’s screen name or user name in connection with internal features or activities.**”*

- Also, paragraph (b) under the definition of “disclose or disclosure” should have the following opening clause:

Subject to paragraph (b) under the definition of “collects or collection”, making personal information collected by an operator from a child publicly available....

- Now that “screen/user name” is a separate item under the definition of “personal information”, we ask the FTC to clarify whether they are still considered “identifiers”
 - This is important for determining whether the wording under paragraphs (g) and (h) of the definition of personal information (i.e., persistent IDs and other identifiers) should be further modified

PERSISTENT IDENTIFIERS AND IDENTIFIERS LINKING A CHILD’S ONLINE ACTIVITIES

General comments

- These two categories are discussed together, as they appear to be addressing the same concern (i.e., “amassing online profiles of children” and “delivering behaviorally targeted ads to children). See pages 37-38 of the FTC proposal.
- **KSP supports the idea of regulating third party behavioral ads in the children’s online space, albeit for a different reason having to do with safety.** We are more concerned with the unpredictability of behavioral ads in terms of their content and the sites to which they link, especially on computers used by multiple members of a family. Although Internet-wide tracking of a child’s computer may be seen as a privacy invasion by some, the safety and content risks associated with these ads pose a much greater concern. Some third party ad networks provide filters for publishers to block certain categories of ads; however, in our experience, these filters have not proven to be effective. For these reasons, third party behavioral ads are not currently allowed under our program guidelines.
- Our industry survey on this point showed that only a small percentage of operators are currently engaged in the practice of third party behavioral advertising (see below). This suggests that the elimination of this practice on children’s sites and online services is not likely to have a

significant impact on industry. **However, the survey results also suggest that other forms of advertising (including contextual ads and ads from third party partners) are still popular.**



Detailed comments

- Because of the internal operations carve out for “persistent identifiers”, it appears that items (g) and (h) under the expanded definition of “personal information” are regulating exactly the same thing (i.e., “online profiling” and “behavioral advertising”). And thus one of two clauses is probably not necessary. In other words, if category (h) is a catch-all category meant to cover all identifiers (including identifiers that are not persistent), it would appear that category (h) alone would be sufficient? In other words, what is category (g) covering that is not already covered by category (h)?
- Regardless, **the current wording of category (h) is much broader than the activities it is trying to regulate** (as per the FTC’s comments on pages 37-38 of the proposal). Plus, the term “different” is not defined, creating greater uncertainty for operators.
- Based on the concerns above, paragraph (h) under the definition of “personal information” should be revised as follows:

*“an identifier that links the activities of a child across different **unaffiliated** websites or online services **for the purpose of creating online profiles of the child or delivering behavioral advertising to the child.**”*

- This revised wording would address the concerns expressed by the FTC, while still allowing operators to engage in a variety of common practices (which pose little or no harm to children), including:
 - Website analytics
 - Website personalization (including tailored content)
 - Tracking across different sites or online services owned by the same company
 - Tracking for first-party advertising/marketing purposes (a distinction the FTC has recognized under its general OBA principles⁵)
 - Tracking for educational progress purposes (a practice now used by several educational toy companies, including LeapFrog, Nickelodeon, PBS, Sesame, etc.)
 - Tracking that is done for a good cause (e.g., using an identifier to track a child’s fundraising activities for a variety of charitable organizations)

⁵ See [FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising: Tracking, Targeting, and Technology \(February 2009\)](#)

- [Tracking for purposes of rewarding children for using multiple kids' sites and online services within an enclosed environment – i.e., kids' browser]
- The phrase that says – “or protection of the security or integrity of” – under category (g) covering “persistent identifiers” is unnecessary and can be removed. This phrase is already included under the revised definition of “support for internal operations”

PHOTOS, VIDEOS, AND AUDIO FILES

- **KSP does not support the change made to this category of “personal information”, as it would likely have a significant and costly impact on industry**
- The proposed change would mean that operators will need to obtain verifiable parental consent before allowing kids to upload (to the web) photos, videos, or audio files that contain a child's image or voice. This would be required even if the file contains nothing more than the child's face or voice and even if the registration associated with the uploading activity does not require any personal information.
 - This issue is compounded by the fact that the FTC is proposing to eliminate Email Plus, which appears to be the most popular method of obtaining parental consent for these types of activities
- Also, the proposed change is likely to have the following unintended consequences:
 - If prior parental consent will be required, kid-friendly companies will be discouraged from developing and providing contests, promotions, and other features (such as tell-a-friend features) that involve the uploading of photos, videos, or audio files
 - As a result, kids will likely turn to other sites and apps (not intended for them), such as Facebook and YouTube, to partake in user-generated activities. This can't possibly be good for kids, especially at a time when we know kids are lying about their age to get onto popular social networks (and with the help of their parents)⁶.
 - Also consider the impact this change will have on mobile devices and mobile apps, which are frequently used by kids to take, upload, and share photos, videos, and audio files with their family and friends? Are app developers expected to obtain verifiable parental consent before these activities can occur? How would this even work at a time when we don't have a mobile-friendly consent mechanism enumerated under COPPA?
- Also, how would you treat images/videos which are blurred or unclear, or caricatures of a child's face? It will become hard to draw the line on what constitutes a valid image or voice, unless the file needed to be accompanied by other identifying information for it to be considered personal.
- Based on the concerns raised above, KSP strongly encourages the FTC to consider one of the following alternatives:
 - Option 1 – Revert back to the original language of this clause, which would require that a “photo, video, or audio file” be combined with “other information such that the combination permits physical or online contacting”
 - Note that the FTC expressed concern about metadata, geo-location, and facial recognition technology. But we believe these issues are already addressed within the existing language. In other words, to the extent that a photo or video is combined with metadata, geo-location, or facial recognition technology (i.e., “other information”) such that it would permit physical or online contacting of a child, then the photo/video would anyway be considered “personal”, even

⁶ See study by Dana Boyd, Eszter Hargittai, Jason Schultz, and John Palfrey (Microsoft Research – Nov 2011): [“Why Parents Help Their Children Lie to Facebook: Unintended Consequences of the ‘Children’s Online Privacy Protection Act’”](#).

under the existing language of the law. The difference, though, is that under the old language, companies would still have the option to remove the “other information” prior to the image/video being stored and thereby avoid the need for verifiable parental consent.

- **Option 2** – Apply the “support for internal operations” exemption to this category of personal information (as was done for other categories). This way, companies who use media files only for internal purposes (but not for posting in a public community area or shared profile page) would not be required to obtain verifiable parental consent (or, at most, would be required to obtain a lighter form of parental consent, such as Email Plus). This is one area (among others discussed below) where the Email Plus consent mechanism could still be very useful.

GEOLOCATION INFORMATION

- **KSP is not necessarily opposed to adding “geolocation information” as a new category under the definition of “personal information”; however, we would recommend that a distinction be made between the collection and use of geolocation information for marketing purposes versus non-marketing purposes**
 - The privacy concerns would appear to be greater when location tracking is being done for marketing purposes (e.g., to send a customized coupon for a store in close proximity to the child) versus it being done for convenience and/or safety purposes (e.g., to allow a parent to track their child’s whereabouts within an amusement park via a mobile app). In the absence of a mobile-friendly parental consent mechanism, requiring verifiable parental consent prior to the collection of this information for *non-marketing* purposes would appear to be overly burdensome, relative to the potential risks.
- For the reasons stated above, we recommend that category (j) of the definition of personal information be revised as follows:

*“Geolocation information sufficient to identify street name and name of a city or town, **when such information is being used for marketing purposes.**”*

COMBINATIONS OF NON-PERSONAL INFORMATION

- The combination of “date of birth, gender, and zip code” should not be considered “personal information”, as there would seem to be numerous individuals who could meet such criteria, even within a particular zip code. Plus, rarely have we seen companies collect ONLY this type of information as part of a registration form. If collected, it is typically collected together with at least one element of personal information, in which case the data would anyway be regarded as personal information. Another consideration is the fact that most companies likely would not be able to decipher who a person is (based on only DOB, gender, and zip) without the assistance of an outside data aggregator.
- ZIP+4 should not be considered the same as a physical address, as most ZIP+4 codes include multiple addresses. In the rare instances where only one address is covered by ZIP+4, it is usually a commercial building rather than a personal home address.

DEFINITION OF “WEBSITE OR ONLINE SERVICE DIRECTED TO CHILDREN”

- The addition of 2 new factors to this definition (i.e., musical content and the presence of child or child-appealing celebrities) is helpful and will provide additional clarity to operators
- **KSP encourages the FTC to consider adding other factors that touch on newer trends**, such as:
 - Whether offline merchandise associated with the site/app is directed toward kids (or sold in toy stores for kids)
 - Whether apps are offered on devices or platforms which are more appealing to kids (e.g., Nook, Kindly Fire, Apple Kids section, LeapFrog LeapPad, Nintendo devices, etc.)
- We also ask the FTC to provide guidance regarding the proper treatment of websites and online services directed toward very young children (i.e., preschoolers), which often have registration forms directed toward parents
 - Are these sites considered “directed toward children” such that they need verifiable parental permission? Or can these sites rely on the expectation that a parent or adult is the one creating an account and therefore verifiable consent would not be required?
 - Is there an age at which a site can presume that a child is too young to register on his/her own? If so, what is that age?

PRIVACY POLICY AND DIRECT NOTICE

- **KSP praises the FTC for attempting to simplify privacy statements and we generally support the new simplified disclosures model**
- However, the FTC does not appear to be applying this model consistently across other areas of the notice requirement. For example:
 - Requiring the identification and contact information of all operators is likely to lengthen privacy statements (not shorten them) and create more confusion for consumers
 - The same is true for the new direct notice requirements, which may result in longer and potentially more confusing notices
- KSP favors a model that is even more bite-size in terms of the information furnished to parents
 - For example, we would support a model that simply requires an operator to highlight the different “features” available on its site or online service (somewhat akin to the model we use on our certification website at www.kidsafeseal.com)
- We also have the following additional requests/concerns regarding the new operator identification requirement:
 - Can this requirement (to list out all operators) be limited to just 3rd party ad networks?
 - As written and based on the existing definition of “operator”, it would appear that this requirement would not apply to vendors collecting and processing information on a website’s behalf. Can the FTC confirm?
 - Would this rule apply to one-time joint sponsors of a promotion who co-collect information on a website? If so, each time a contest of this kind is run, the privacy policy would have to be updated, and then when the promotion ends, updated again. This would create an unreasonable burden on companies. It would seem much more effective to communicate the participation of multiple companies directly on the pertinent registration form, rather than in a privacy policy which few parents ever read.

This approach would also seem to be more in line with the principle of “Greater Transparency” under the FTC’s new privacy framework.⁷

- It would be helpful if the FTC created and published examples of COPPA-compliant direct notice communications. Although these notices tend to be contextual, a sample model for each direct notice scenario would be useful for industry **and would help create a standardized template that parents can expect to receive.**
- In regards to the placement of privacy policies within mobile apps, we make the following suggestions:
 - We do not recommend placement where the app is purchased or downloaded, as this area tends to be loaded with descriptions about the product. A privacy notice on this page would likely be blended in with other content and go unnoticed.
 - We also do not necessarily recommend placement of a privacy policy “hyperlink” within the mobile app itself, as many developers of childrens’ apps prefer to keep their app environment web-free
 - The most ideal placement would appear to be within the “info” or “terms” section of a mobile app or within a separate section/tab created just for the privacy policy. For this to be practical, however, the disclosure requirements would have to be further simplified to accommodate viewing on a small screen.

VERIFIABLE PARENTAL CONSENT

Elimination of Email Plus

- **KSP does not support the elimination of Email Plus as a recognized consent mechanism**
- We are greatly concerned about this change for the following reasons:
 - The FTC verbally acknowledged that the decision to remove email plus was not based on any finding that children were being harmed as a result of this consent mechanism
 - **This change would eliminate the only automated and highly-scalable method of parental consent available today**
 - This change will cause considerable cost to industry, requiring many companies to overhaul the configuration of their website registration processes
 - Note that the FTC’s estimates of costs to industry are based on hourly fees which are appear to be way below industry standard rates for expertise in these areas
 - **This change will likely cause a significant reduction in the range of fun online activities made available to kids. Kids will be locked out of even more activities.**
 - We all know that over the years COPPA has caused many “kid-appealing” sites to up the minimum age requirement to 13, mainly for the sake of avoiding the burden of COPPA compliance. This trend will likely continue and even grow if Email Plus is removed from the set of parental consent options.
 - We don’t agree that the removal of Email Plus will help spur innovation. Quite the contrary. **We’re fearful that the removal of Email Plus will freeze innovation, as companies are likely going to try avoiding COPPA entirely, instead of trying to devise new more-reliable ways for obtaining parental consent.**
 - It is worth noting that Email Plus (even if not reliable enough for parental consent) offers one ancillary benefit – it requires a double opt-in process for the verification of an

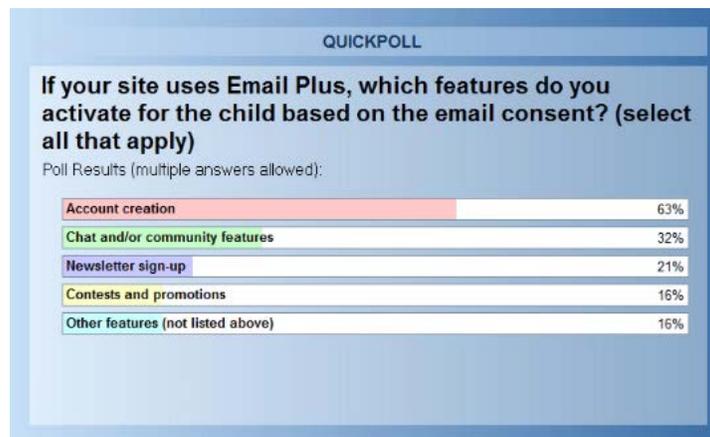
⁷ See [Preliminary FTC Staff Report \(Dec 2010\) – “Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers”](#)

email address, and so it provides a level of data integrity which is important for the collection of parents and/or kids' information.

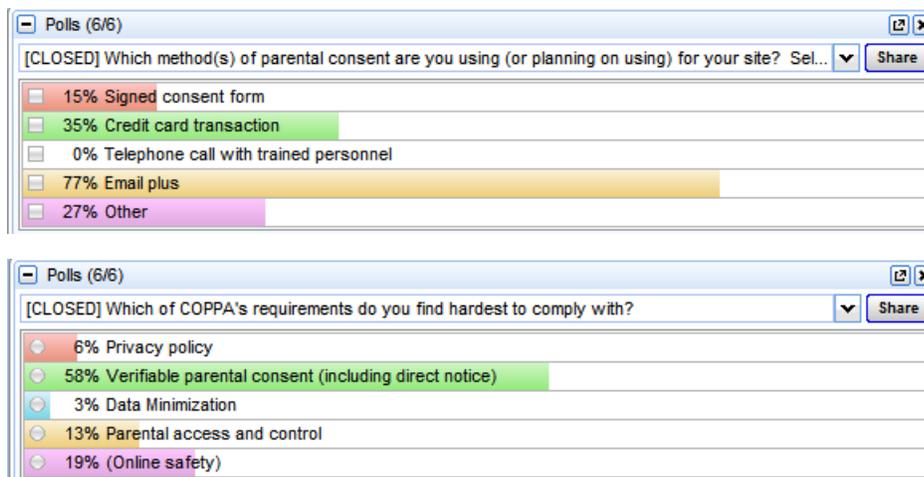
- **Overall, we agree that Email Plus is generally a less reliable method of consent, but there are still too many scenarios where it is essential to have Email Plus as a parental consent option.**
- Take for example the following (all of which are popular practices on kids' websites today):
 - Scenario 1 – a website wishes to collect a parent's email address during registration and use it for multiple purposes (e.g., to notify the parent about the child's account, to send the parent periodic newsletters, etc.). With the proposal changes to the COPPA Rule, this practice would not be allowed, even if each of the uses above – by itself – followed the procedures of the corresponding parental consent exception. The site would not be allowed to collect the parent's email address for both of these uses at the same time, unless the site obtained a more reliable form of parental consent. But should a full-fledged verifiable parental consent process be required in this scenario (simply because two relatively harmless uses directed at the parent were bunched together)? Or should this kind of practice be authorized with a lighter Email Plus consent mechanism?
 - See separate discussion about this scenario later, under the section titled "[EXCEPTIONS TO PARENTAL CONSENT](#)" – Exceptions #2
 - Scenario 2 – what about a newsletter sign-up form which desires to collect slightly more information than just a child's email address (perhaps also a zip code or the child's gender so that the newsletter can be slightly customized)? Should something this simple and relatively harmless warrant the need for a more sophisticated and cost-prohibitive consent mechanism?
 - Scenario 3 – what about a contest or promotion that involves the collection and internal review/usage of non-identifiable photos or videos? Should this require an elaborate consent mechanism?
 - Scenario 4 – What about a Customer Support feature, which typically requires that kids provide an open-ended description of their customer support issue, in addition to a contact email address? Shouldn't something relatively this harmless be acceptable under Email Plus or perhaps no consent mechanism at all?
 - See separate discussion about this scenario later, under the section titled "[EXCEPTIONS TO PARENTAL CONSENT](#)" – Exceptions #4 and 6
- The examples above illustrate that currently there's too much of a gap between the limited activities that can occur under the parental consent exceptions and all other activities (which would necessitate an elaborate consent process)
- **Based on the concerns above, we urge the FTC to preserve Email Plus as a valid consent mechanism. To the extent the FTC is still concerned about its reliability, we would suggest that the method be preserved at the very least for some or all of the following purposes:**
 - Email Plus could be used to authorize activities that slightly exceed the limitations of the parental consent exceptions but that do not rise to the level of extensive collection or use that would require a more reliable form of consent (see scenarios above)
 - Although children's data may be considered "sensitive", there are certainly certain types of children's data (such as "email address") which are arguably less sensitive than others (such as "physical home address")
 - Email Plus could be used to authorize activities that involve the use of multiple parental consent exceptions at one time (see scenarios above)

- Perhaps Email Plus can be used as a full-fledged consent mechanism for children under the age of 8, as these younger children are less likely to have their own email addresses or the knowhow to circumvent the parental consent process
- Perhaps most important of all, email plus could be used as a best practice for sites and online services seeking to keep parents informed and involved, even when legally they're not required to do so
 - We're convinced that the removal of Email Plus will result in parents being less notified of their children's online activities. This is because, in the absence of Email Plus, companies may strive to squeeze every ounce out of the parental consent exceptions, or design their online features so that no personal information is collected at all, resulting in parents being generally less aware of which sites on the web their children are interacting with.
- To further illustrate our concerns regarding the removal of Email Plus, we'd like share with you the results of several industry surveys we've conducted on this point. **As you can see, Email Plus is still very popular, and its removal will clearly have a considerable impact on industry.**

December 2011



June 2010

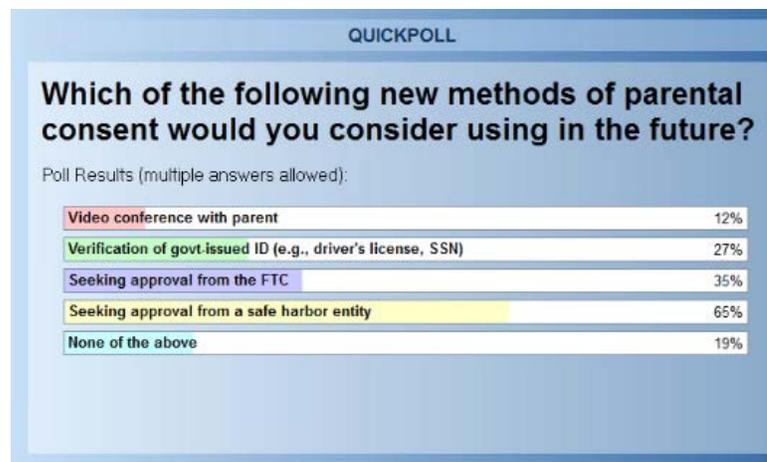


Other Consent Mechanisms

- Although we’re skeptical whether the new enumerated methods (e.g., video based consent, govt. ID verification, etc.) will be widely used, we support the addition of these new methods
- KSP believes it would not be unreasonable for operators to be required to maintain records of parental consents, as this is practice is already being followed by many companies. However, it is likely much easier to records these consents when the consent mechanism is automated.
- In regards to the consideration of other parental consent techniques, KSP is curious why the iTunes-based model was rejected by the FTC? If there’s a credit card tied to virtually every iTunes account, then when someone types in their password to download an app, shouldn’t this action be just as good as a credit card transaction, especially when there’s a charge for downloading the app? Similar to a credit card transaction, if the child makes the app purchase on his/her own, the parent will be notified of the transaction via an email receipt from Apple.

New Procedures for Approval of New Consent Methods

- **We strongly support the addition of two new procedures for approval of consent mechanisms (i.e., via the FTC and safe harbor entities)**
 - In fact, our industry survey on this topic suggested that the new approval procedures are likely to be popular, especially the safe harbor option (see below). This may drive more companies to participate in safe harbor programs.



- **Despite our support, we believe the new approval procedures and the benefits of each need to be more clearly defined.** For example, we raise the following questions:
 - What is the benefit of the FTC’s approval over the safe harbor’s approval? Does the approved method become an enumerated method if approved by the FTC? Is anyone likely to consult the FTC if it takes up to 6 months to approve, with no guarantee of approval? It would appear this timeframe should be shorter (maybe 3 months at most).
 - If the FTC does not agree with a safe harbor’s decision, will it have veto power (and would operators be expected to change their practices)? This would obviously create an unreasonable burden for operators.

- Will safe harbors be able to consult the FTC regarding approval requests?
- Will safe harbors be expected to document their evaluations and decisions in writing?
- The words “in good faith” should be added to the safe harbor portion of this new section in order to protect safe harbor programs for trying their best in making approval decisions
- Based on the comments above, we recommended the following revisions to Section 312.5(b)(4):

*“A safe harbor program...may approve its member operators’ use of a parental consent mechanism not currently enumerated in paragraph (b)(2) where the safe harbor program (i) determines **in good faith** that such parental consent mechanism meets the requirements of paragraph (b)(1) **and (ii) documents the basis for its determination.**”*

EXCEPTIONS TO PARENTAL CONSENT

General comments

- **Several of the changes to the parental consent exceptions are problematic and some of the existing wording can be improved.** Also, across all of the exceptions, the limitation on allowing only the use under that particular exception (and no other uses) will be extremely burdensome, based on what operators are doing today. We further address all of the exceptions below.

Detailed comments

- Exception 1 (exception for obtaining parental consent):
 - Collection of a child’s email address should be allowed under this exception, as it provides the only means for the operator to notify the child when the parent’s consent has been received. If a child’s email is allowed under exception 4 (i.e., the multiple-contact exception), it should be allowed here too.
 - The term “reasonable time” should be defined. Industry practices vary widely here. KSP recommends a period of at least 14 days.
- Exception 2 (new) (exception for notifying parent about child’s participation):
 - As written, this exception would only be available if the site or online service does not collect personal information from kids ANYWHERE ELSE ON THE SITE. This limitation does not seem right, and would appear to be inconsistent with the FTC’s intentions. Perhaps when referring to “no other collection”, the FTC meant that no other personal information can be collected for the specific activity/feature that the parent is being notified about. Regardless, this limitation should be removed
 - The second sentence of this exception is also problematic, as it would mean that a site would not be allowed to use the parent’s email address (collected lawfully under this exception) for another purpose (such as newsletters), even if the operator followed one of the other exceptions (i.e., exception 4) to authorize that extra use.
 - Based on the concerns above, this new exception (i.e., Section 312.5(c)(2)) should be revised as follows:

*“Where the sole purpose of collecting a parent’s online contact information is to provide notice to, and update the parent about, the child’s participation in a website or online service ~~that does not otherwise collect, use, or disclose children’s personal information.~~” In such cases, the parent’s online contact information may not be used or disclosed for any other purpose, **unless such other purpose conforms with a separate exception under this Section 312.5(c) or otherwise complies with Sections 312.5(a) and (b).**”*

- The language stricken above also needs to be removed from Section 312.4(c)(2)(i) – the direct notice clause. A change may also need to be made to 312.4(c)(2)(ii) to reflect the red language above.
 - Page 73 of the FTC’s proposal (top of page) suggests that the exception above also does not allow the combination of a parent’s online contact information with other information about the child, although this wording does not appear in the wording of the law itself. The FTC should clarify that this was an error in the federal register notice. Clearly, the parent’s email address would need to be combined with the child’s account information for the operator to know when to send an update to the parent about the child’s activities and which email to send it to.
- Exception 3 (one-time-use exception):
 - The changes to this exception are reasonable. We have no further comments.
- Exception 4 (multiple-contact exception):
 - The FTC should consider allowing operators to combine one or two other pieces of non-personal information to a child’s email address under this exception, especially if the Email Plus consent mechanism is eliminated from the law. In the case of newsletters, examples of extra information may include child’s “first name” or “username”, “zip code”, and/or “gender”. This would allow for a small (but meaningful) amount of personalization, without having to get full-fledged verifiable parental consent. Also note that collecting additional pieces of information can sometimes help verify the accuracy and integrity of the email addresses being collected.
 - Also, to the extent that this exception is used for purposes of providing customer or technical support to a child, it is essential that the operator be allowed to ask for additional information regarding the issue the child is having. Operators cannot be expected to provide adequate customer support to users without this additional information. **That said, we believe an entirely separate exception (akin to exception #5 below) should be created just for customer support features, or at a minimum, customer support should be added under exception #6 (see below).** Customer support is a common feature on kids’ websites and should not require prior verifiable consent.
- Exception 5 (safety exception):
 - An operator should be allowed to collect a “parent’s name” in addition to the “child’s name” as this may help in further resolving the issue and ensuring that the parent contacted is in fact the parent of that child
- Exception 6 (security/legal exception):
 - Unless a separate stand-alone exception is created for customer support features, this exception should be expanded to also include customer support:

*“Where the sole purpose of collecting a child’s name and online contact information is to: (i) protect the security or integrity of its website or online service **or the security of its users**; (ii) **provide customer or technical support**; (iii) take precautions against liability; (iv) respond to judicial process; or (v) to the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety; and where such information is not ~~be~~ used for any other purpose.”*

- All of the comments regarding the exceptions above become even more critical if Email Plus is eliminated as a consent mechanism. In other words, we need to give operators the ability to combine the use of several exceptions at one time if they will no longer have the ability to use Email Plus to authorize multiple activities.

PARENTAL ACCESS AND CONTROL

- **Although this section of the COPPA Rule has not been modified, we ask the FTC to consider how this requirement will apply to the new categories of “personal information”**
- For example, how would operators realistically be expected to give parents access to:
 - IP addresses (plus other identifiers) when used for non-internal operations
 - Geo-location information
 - Photos, videos, audio files
- It would seem more plausible to limit the access requirement to information that operators can realistically present to a parent (things like “email address”, username and password, etc.)

CONFIDENTIALITY AND SECURITY

- In regards to the new due diligence requirement for vendors and third parties, we have the following comments:
 - With the expanded definition of “personal information”, there could be many more vendors and third parties that would need to be vetted under this new requirement
 - The cost of compliance in this area (although perhaps justified) may be significant, as these types of reviews tend to involve the use of outside lawyers and consultants
 - Also note that smaller companies may face challenges in complying with this requirement. For example, picture a small startup website trying to negotiate security clauses with a service provider such as Google.
 - **In light of the concerns above, the FTC should consider applying this requirement on a go-forward basis only**
 - The FTC should also provide guidance around what steps (at a minimum) might be considered reasonable for performing this type of due diligence

DATA RETENTION AND DELETION

- **KSP encourages the FTC to consider how the new data retention and deletion requirements can will be applied to the new categories of personal information, including identifiers**
 - As part of this, consider whether the deletion of identifiers will even be within the control of operators (versus an ad network or mobile platform such as Apple)
- **Also, the wording of this new clause is problematic for several reasons:**
 - Limiting storage to only as long as necessary for the original purpose is not reasonable. Operators must be allowed to store personal information for longer, as they may have legal or business obligations to do so. For example, they may need to preserve records to comply with contests/sweepstakes laws and to meet records retention requirements for customer complaints, technical support issues, and safety issues. For this reason, assigning specific time frames to this clause is not recommended
 - The sentence about deletion is worded awkwardly, and appears to assume that data has to be deleted. Instead, what the clause is really saying is that if there is data being deleted (or required to be deleted), then the deletion has to be done securely.

- Based on the concerns above, we propose revising Section 312.10 as follows:

*“An operator of a website or online service shall retain personal information collected online from a child for only as long as reasonably necessary to fulfill the purpose for which the information was collected **or for other legitimate business or legal purposes. When deleting personal information no longer needed, the operator must take reasonable measures to protect against unauthorized access to or use of the information being deleted.**”*

- It would be helpful to have guidance on what are considered “reasonable measures”⁸

SAFE HARBOR PROGRAMS

Requirement to provide more detailed information in safe harbor applications

- **KSP supports this change and believes more detailed information during the application process will give the FTC greater comfort regarding the operations of safe harbor programs**
 - However, safe harbor applicants must be assured that business model information will be kept confidential by the FTC
 - Also, applicants should not necessarily be required to utilize technological mechanisms for overseeing member compliance. In our experience, manual procedures can be equally or more effective.
 - For example, consider the fact that many kids’ virtual worlds are run in Adobe Flash, and currently there are few (if any) automated tools that can effectively scan and monitor compliance inside Adobe Flash
- KSP requests that this new requirement be applied to existing safe harbor programs, in addition to new applicants

Requirement to assess members annually

- **KSP supports this requirement, as we believe assessments must be conducted at least annually in order to keep up with the changes made by operators**

New reporting requirements

- **KSP supports the idea of the FTC having some level of oversight over safe harbor programs, but not to the extent currently proposed**
- Our concerns and recommendations are as follows:
 - **Safe harbor programs should not be required to report the results of individual member assessments**, as this may discourage operators from participating in safe harbor programs. Instead, we would support an aggregate reporting model whereby safe harbors would be required to report general compliance statistics. We believe this model is also favored by some of the existing safe harbor entities.
 - We also do not believe safe harbors should be required to report violations to the FTC immediately upon discovery (for the same reasons above)

(continued on next page)

⁸ The FTC may wish to consult the data deletion requirements under the FACT Act.

- Based on the concerns above, we propose the following modifications to Section 312.11(d):

(1) *Within one year after the effective date of the Final Rule amendments, and every eighteen months thereafter, submit a report to the Commission containing, at a minimum, a **non-identifiable overview** of the results of the independent assessments conducted under paragraph (b)(2), a description of any **material** disciplinary actions taken against ~~any~~ subject operators under paragraph (b)(3), and a description of any approval of members operators' use of a parental consent mechanism, pursuant to Section 312.5(b)4;*

(2) *Promptly respond to **reasonable** Commission requests for additional information **regarding the program's compliance with the safe harbor requirements**;*

(3) *Maintain for a period not less than three years, and upon **reasonable** request, make available to the Commission for inspection and copying: (i) Consumer complaints alleging **material** violations of the guidelines by subject operators; **and** (ii) Records of **material** disciplinary actions taken against subject operators. ~~and (iii) Results of the independent assessments of subject operators compliance required under paragraph (b)(2).~~*

- In regards to the reporting requirement, we would ask the FTC to provide a template format in which it would like to receive this report, so that all safe harbors can report their findings in a consistent manner
- Also, we believe submitting reports every 18 months is reasonable (and do not recommend a shorter timeframe)

TIMELINE FOR FINAL RULE

In regards to industry implementation of the new COPPA Rule, and regardless of the specific changes that ultimately become final, we urge the FTC to consider the following recommendations:

- **Any and all changes should be applied on a prospective basis only.** Operators should not be expected to get verifiable parental consent for data collection activities that occurred in the past. Applying the new COPPA standards retroactively would create a major burden on industry and likely confuse consumers/parents who need to be contacted about the new requirements.
- **The changes should not be effective immediately, and should have a phase-in period of at least 6-9 months to allow ample time for operators to design new data collection procedures (as necessary).** Many companies use outside agencies to run their websites and online services, and these agencies are likely to charge a lot of money and take a long time to implement the new requirements.

Given what's at stake and to help ensure that industry can handle a revised COPPA Rule, we urge the FTC to consider creating an advisory group of industry experts who can help the FTC further explore and assess the true impact the proposed changes will have on industry, especially in areas such as mobile where the application of COPPA has not been fully vetted and could pose significant practical challenges.

We look forward to next steps in the evolution of the COPPA Rule, and, again, invite you to contact us with any follow-up questions or inquiries.