John P. Tomaszewski, Esq.
General Counsel & Corporate Secretary
johnt@truste.com

December 15, 2011

Federal Trade Commission
Office of the Secretary
Room H-113 (Annex E)
600 Pennsylvania Avenue N.W.
Washington, DC 20580

By Online Submission to: https://ftcpublic.commentworks.com/ftc/2011copparulereview/

Re: TRUSTe Comments to COPPA Rule Review, 16CFR Part 312, Project No. P104503

TRUSTe appreciates the opportunity to comment on the proposed amendments to the Children's Online Privacy Protection Rule ("COPPA Rule" or "Rule"). TRUSTe has been a FTC-approved COPPA safe harbor since 2001, and has witnessed the technological changes that the Commission references in its summary statement. We agree that the COPPA Rule should be amended to address these technological changes and that the proposed Rule changes are positive steps to streamline and provide clarity to the COPPA Rule.

We have provided specific responses to questions raised in the FTC's request for comment. In addition, we'd like to emphasize the following points:

1. *COPPA Rule changes impact both companies and end users* - It's important to assess the impact of all COPPA Rule changes from the perspective of companies that must comply, and end users (children and their parents) that might be impacted.

2. *Identifying multiple operators will remain a challenge for compliance with the Rule* - One of the significant technological changes that have impacted the COPPA Rule is the rise of online services available through an expanded array of computing devices. As a result, it is often difficult to identify which entity is the operator responsible for providing parental notice and obtaining consent. For example, including identifiers used to link the activities across different websites or online services as personal information may increase the number of instances where there will be multiple operators on a single website or online service.

3. *Industry incentives are important to promote "Privacy by Design" within a compliance framework* - TRUSTe supports the Commission's efforts to encourage "Privacy by Design" through innovation around parental consent mechanisms. TRUSTe recommends giving industry incentives to develop alternative forms of direct parental consent and privacy notices by extending the proposed Rule changes around approving alternative forms of parental consent mechanisms to also include direct parental consent and privacy notices.

4. *The COPPA Rule is strengthened by accountability and other proposed data management provisions* - TRUSTe is pleased to see the addition of accountability, security, data retention, and data management processes, as these are key components to any effective privacy program. However, there are challenges around requirements

regarding data retention and deletion being too specific or prescriptive. Providing specifics around data retention timeframes could potentially conflict with the operator's other legal obligations.

5. *The COPPA safe harbor program is strengthened by additional requirements for safe harbor programs* - Operators need to be accountable to their stated privacy promises and meet program requirements of any approved safe harbor program in which they participate. Approved safe harbor programs must also be accountable around how they administer their programs. Additional criteria for safe harbor approval, reporting around program compliance, and requiring annual recertification are important. Such criteria will further demonstrate why COPPA safe harbors serve as a model for other types of safe harbor programs, and why these types of program are effective.

To respond to the Commission's questions, TRUSTe has provided use case examples, along with specific recommendations that address each of the five key areas of proposed Rule changes:

1. Definitions
2. Notice
3. Parental Consent
4. Data Retention and Deletion
5. Safe Harbors

1. Definitions

Question 4: Are there identifiers that the Commission should consider adding to the list of "online contact information"?

TRUSTe supports the addition of "geo-location" data to the definition of personal information. Under its Privacy Certification program, TRUSTe classifies geo-location data as sensitive personal information.[1] TRUSTe's program requirements define geo-location data as "information obtained through an Individual's use of a Mobile Device and is used to identify or describe the Individual's actual physical location at a given point in time." A key component of this definition is the qualifier "actual physical location" that references the technical capabilities of the device to pinpoint the actual physical location of an individual.

We believe it is important to qualify the definition of geo-location data to differentiate it from other types of location data, depending on the ability of the device or software to pinpoint actual physical location. For example, certain geo-location information, such as a zip code, may not reflect a child's actual location. Location identifiers, such as address, city, and zip code that are directly provided by the child are already covered under the definition of Personal Information under the Rule. What is not currently reflected in this definition is the ability of certain data, such as geo-location data, to identify the child's precise location.

TRUSTe recommends that the Commission amend the definition of "Personal Information" under the Rule as follows:

Personal information means individually identifiable information about an individual

[1] TRUSTe, Program Requirements, 18 Nov. 2011, http://www.truste.com/privacy-program-requirements/program-requirements.

collected online, including: …

(j) Precise geo-location data that can be used to identify a Child's actual physical location at a given point in time.

TRUSTe has determined it prudent to describe personal information in a more effects-based mode, rather than attempting to describe what specific data points constitute personal information. Much of this approach is based on the observation that data may or may not be personal information depending on the context of the data relative to other data (or meta-data). In addition to the example noted above, depending on the actual value of the data, it may be personal information in one context where it is not in another (e.g. first name, last name, ZIP may be personal information if the specific ZIP only has one combination of first and last name).

Question 5: Proposed § 312.2 would define personal information to include a "screen or user name."

a. *What would be the impact of including "screen or user name" in the definition of personal information?*
b. *Is the limitation "used for functions other than or in addition to support for the internal operations of the website or online service" sufficiently clear to provide notice of the circumstances under which screen or user name is covered by the Rule?*

The above-referenced changes to the Rule, including the limitations around "used for functions other than to support for the internal operations of the website or online service," do not effectively reflect current uses of screen or user name by a single operator and do not provide sufficient notice of when screen or user names are covered by the Rule. The following use cases demonstrate why:

1. A single operator operates multiple websites or online services that are integrated in such a way that a child can easily navigate from one website or online service by only having to login once. Information collected from the child includes screen or user name and password, and the operator's privacy policy is the same across all the websites or online services. Will the operator need to obtain parental consent for the child to access each website or online service? What impact would this have on the end user experience?

2. A single operator offers mobile optimized versions of its PC website or online service. The operator offers a mobile application that utilizes the same screen or user name the child uses to access the website or online service on the desktop web. The child's activities are synched up regardless of which device she or he uses to access the website or online service. For example, if a child is playing a game on a laptop and later logs into the game through the mobile app, the child will pick up where she left off, and content is displayed based upon her settings. Will the parent only need to provide consent once so that consent will apply to all forms of a website or online service regardless of how it is accessed (e.g. website or mobile application)?

3. An operator operates a website or online service that enables children to connect with each other in virtual worlds. The child is asked to create a screen name so they can chat with others in the virtual world. The chat function filters out words considered to be personally identifiable. Along with screen name the operator collects age and gender to allow the child to customize her avatar and to place the child into age appropriate worlds

to ensure the child is chatting with others her own age. Will screen or user name be considered personal information if combined with other non-personally identifying information such as age and gender? This may impact an operator's ability to segregate users into age appropriate groups, and may also complicate its ability to provide personalized online experiences.

4. A web-connected gaming console enables gamers, including children, to play against each other, chat, and post high scores. Players are recognized by screen or user name. The game's chat function filters out words considered to be personally identifiable. The screen or user name is used for all games available for that gaming console. Will the web-connected gaming console -where a screen or user name is used within a single gaming console but across multiple games - be considered a single online service, or will the games that the child plays each be considered a separate online service?

The Commission notes in its discussion that while screen and/or user names are becoming increasingly portable, the addition of screen or user names to the definition of personal information does not effectively address the issue of portability.[2] Operators offering a suite of related websites or online services that utilizes a single screen or user name throughout the service offerings intend the child to only be recognized within that suite of services so the child may have a seamless online experience. TRUSTe believes placing restrictions around providing a centralized registration and login across all services will provide a poor online experience. TRUSTe recommends modifying when a screen or user name is personal information to address the use case noted in the Commission's discussion - the case of being able to identify a child by screen or user name across multiple services provided by multiple operators.

The Commission should also consider expanding the definition of website or online service to include a set of websites or online services integrated through a common registration or login process offered by a single operator.

Question 6: Proposed § 312.2 would define personal information to include a "persistent identifier."

a. What would the Impact of the changes to the term "persistent identifier" be in the definition of personal information?

b. Is the limitation "used for functions other than or in addition to support for the internal operations of the website or online service" sufficiently clear to provide notice of the circumstances under which a persistent identifier is covered by the Rule?

Persistent identifiers differ from screen or user name because a screen or user name is something that is typically created by the user. A persistent identifier is an identifier that is automatically created by the party setting the identifier such as an IP address or a number contained in a cookie. A screen or user name identifies an individual, whereas a persistent identifier identifies a browser or a device. We think that this is an important distinction when considering whether persistent identifiers should be classified as personal information. We also

[2] "Data Portability Definitions," Data Portability Project, 21 Nov. 2008, 12 Dec. 2011, http://wiki.dataportability.org/display/archive/DataPortability+Definitions and Christian Scholz, "What is Data Portability," mrtopf.de, 12 March 2008, 12 Dec. 2011, http://mrtopf.de/blog/data-portability/what-is-data-portability/

believe that including persistent identifiers in the definition of personal information will hinder a single operator's ability to offer users rich online experiences. The following use cases illustrate this proposition:

1. An operator may use a persistent identifier (e.g. GUID) to track a child-user within its websites and online services. This tracking enables the operator to maintain the child's session (e.g. recognize logins, etc.), personalize the child's experience, and gather analytics about which areas of the websites or online services are used. The tracking is limited to the websites and online services offered by that single operator, and does not track the child's activity after she navigates to a web site or online service offered by another operator.

   The operator may use a third party analytics service to track web site or online service use as described in the above paragraph. Will the third party analytics service also be classified as an operator if it is only tracking usage activity within a group of websites or online services offered by a single operator? We think that tracking by an operator, or a third party acting on behalf of the operator, across a group of multiple websites or online services provided by the same operator, is not sufficiently addressed in the proposed change to the term "persistent identifier."

2. An operator may also use a persistent identifier to recognize a child-user when they access the website or online service from different devices such as laptop, tablet, or smartphone. The operator is able to offer the child a seamless experience, displaying content based upon the child's set preferences, or to display the last game level the child was playing so she can pick up where she left off. Using an identifier to provide a seamless online experience when accessing the same website or online service through different devices needs to be addressed.

TRUSTe recommends that persistent identifiers not be included as part of the definition of personal information, but be defined separately. A persistent identifier by itself is not personal information as it does not allow you to contact a discrete individual but rather is assigned to a device or similar technology. However, when a persistent identifier is combined with other data that allows for the identification and contacting of a discrete individual, then the combined data may be personally identifiable.

The standalone definition of persistent identifier should include language stating that if the persistent identifier is combined with other data that enables the online contacting of a child, that combined data is personal information.

Question 7: Proposed § 312.2 would define personal information to include "an identifier that links the activities of a child across different websites or online services." Is the language sufficiently clear to provide notice of the types of identifiers covered by this paragraph?

TRUSTe agrees that tracking a child's activities across different websites or online services over time for the purpose of serving the child behaviorally targeted advertisements, or to build a profile about the child that is made available to third party marketers warrants a greater level of privacy protection. As with others in the industry, we recognize that information collected from

children is sensitive and requires greater protections. [3] If entities engage in online behavioral advertising directed to children, and they have actual knowledge that these children are under the age of 13, those entities must comply with the COPPA Rule as well as guidance from the FTC's Self-Regulatory Principles for Online Behavioral Advertising: Tracking, Targeting and Technology.

Classifying "an identifier that links the activities of a child across different websites or online services" as personal information will serve to provide a poor user experience for both children and parents, and will not provide greater privacy protections.

An example would be a website or online service offering free games for children that does not collect personal information, but partners with a third party analytics provider to collect aggregated data about its users including how the user got to the website or online service, and where the user went after they left the website or online service . To collect the data, the analytics provider uses an identifier to gather the information. Under the proposed definition, the analytics provider would be required to obtain parental consent prior to collecting information from the child. This scenario raises some questions:

1. Is the analytics provider an operator? In some cases the identified third party operator will not have a direct relationship with or explicitly request personal information from consumers. In these cases, the first party operator is responsible for obtaining parental consent since the first party has the direct relationship. It's not appropriate for the third party to insert themselves between the consumer and the first party operator.

2. Will the parent need to provide new consent each time a new "operator" appears on a website or online service?

3. What would the notice – consent experience look like in the case of multiple operators? Will each "operator" have to ask the child for the parent's email address for the purpose of sending notice and obtaining consent? This will require companies that traditionally do not have a direct relationship with users, or who have not requested personal information directly from a user, to now collect personal information from a child. Additionally this could be cumbersome in the case of a mobile device. The third party should be allowed to rely on the consent obtained from the first party operator where the third party is "operating" under the direction of the first party.

4. How would consent be tracked? This would raise issues similar to those raised around honoring opt-outs. In a cookie-based system, if a child or parent clears their cookies or uses in-private browsing, the child and parent's preferences, including parental consent are removed. Would this retrigger notice-consent?

TRUSTe recommends that the Commission does not add include "an identifier that links the activities of a child across different websites or online services" to the definition of personal information, because this type of identifier does not identify a discrete child. It is when this data is combined with other data from third party sources that permits the identification of a child. Linking activities across multiple sites identifies a browser or device. Also, this should not be

[3] The DAA's OBA principles, based on the FTC's own Self-Regulatory Principles for Online Behavioral Advertising: Tracking, Targeting and Technology exemplify this approach. "About the Self-Regulatory Principles for Online Behavioral Advertising," 18 Nov. 2011 http://www.aboutads.info/obaprinciples.

added for the reasons cited above. Trying to meet this standard is a risk operators most likely will be reluctant to take on, and would likely chill innovation.

Question 8: Proposed § 312.2 would define personal information to include "photograph, video, or audio file where such file contains a child's image or voice" and no longer requires that photographs (or similar items) be combined with "other information such that the combination permits physical or online contacting." What would be the impact of expanding the definition of personal information in this regard?

This proposed change will impact social sites that enable children to communicate with others using a screen name, without the collection of any other identifying information, and offer features that allow the child to upload user generated content.

Operators that allow children to upload user-generated content under the current rule exception will need to provide notice and obtain consent prior to allowing the further uploading of user-generated content. It is unclear whether the operator will need to remove user-generated content uploaded under the current Rule, where no other identifying information is associated with that content, or whether that material would be grandfathered in.

TRUSTe agrees biometrics such as those provided in a photo, video, or audio recording are personal information and greater protections need to be provided in light of technologies such as facial recognition technology services becoming more widely available. TRUSTe recommends that notice and consent be provided on a going-forward basis. User generated content uploaded by a child prior to release of a final updated Rule should be grandfathered under the current Rule thus not requiring operators to delete the content.

Question 9b: Does the combination of date of birth, gender, and zip code provide enough information to permit the contacting a specific individual such that this combination of identifiers should be included as an item of Personal Information?

Studies have shown that the combination of date of birth, gender, and zip code can identify a discrete individual.[4] However, much of these three data points capability to be personal information depends on the context of the data. These three data points usually need to be combined with data from another source in order to contact that discrete individual.

Operators collect date of birth, gender, and zip code to provide a personalized experience for their users. For example, operators providing services that enable children to connect and interact with each other collect this type of data, along with screen or user name, to allow the child to create a profile so the child can interact with others that are of similar age and share similar interests.

Combining information collected from the child with another piece of information that the operator uses to contact the child or the child's parents should be added to the definition of personal information along with an exception around providing requested services. If the Commission adds date of birth, gender, and zip code to the definition of personal information, TRUSTe recommends the added subsection of the definition to read:

[4] Prof. Paul Ohm, "Public Comment to the Federal Trade Commission, Re. COPPA Rule Review P104503," University of Colorado Law School, 30 June 2011, 18 Nov. 2011, http://www.ftc.gov/os/comments/copparulerev2010/547597-00040-54850.pdf.

"date of birth, gender, and zip code combined with an identifier and where such combined information is used for functions other than or in addition to support for the internal technical operations of the website or online service".

Question 9c: Should the Commission include "Zip + 4" as an item of Personal Information?

"Zip + 4" by itself is not enough to identify a discrete individual and would need to be combined with other data points to identify, locate, or contact an individual and should not be added to the definition of personal information.

Question 11a: Is the term "activities to maintain the technical functioning" sufficiently clear to provide notice of the types of activities that constitute "support for the internal operations of the website or online service"? *For example, is it sufficiently clear that the mere collection of an IP address, which is necessary technical step in providing online content to web viewers, constitutes an "activity necessary to maintain the technical functionality of the website or online service"?*

The term "activities to maintain the technical functioning" does not take into consideration third party services that may be used to assess usability of the website or online service such as understanding how individuals interact with a website or online service (e.g. analysis of which areas or features are most popular, etc.).

TRUSTe recommends the Commission re-assess the definition of "support for the internal operations of website or online service" as this definition is limiting and does not effectively define what is meant by "support for the internal operations." It is unclear why "or to fulfill a request of a child as permitted by §§ 312.5(c)(3) and (4)" is called out specifically in the definition and the other allowable exceptions permitted under §§ 312.5(c) or services the parent has consented to are not included.

The Commission should consider revising the definition to read

Support for the internal operations of the Web site or online service means those activities necessary to maintain the technical functioning of the Web site or online service, to protect the security or integrity of the Web site or online service, or to fulfill a request of a child as permitted by § 312.5(c), and the information collected for such purposes is not used or disclosed for any other purpose either by the Operator or a person who provides support for the internal technical operations of the Web site or online service.

2. Notice

Question 12: Do the proposed changes to the "notice on the website or online service" requirements in § 312.4(b) clarify or improve the quality of such notice?

TRUSTe supports the Commission's goal of streamlining the requirements around notices to parents, as well as making the notices easier for parents to read and understand. TRUSTe agrees with the Commission's proposal to remove the requirement around operators having to state "that the operator may not condition a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity" (§ 312.4(b)(2)(v)). This is a practice an operator should be required to comply with rather than a required disclosure.

However, the proposed changes to § 312.4(b) do not clarify or improve the quality of the notice, specifically:

> *(1) **Each** operator's contact information, which at a minimum, must include the operator's name, physical address, telephone number, and email address;*
> *(2)A description of what information **each** operator collects from children, including whether the website or online service enables a child to make personal information publicly available; how such operator uses such information, and; the operator's disclosure practices for such information; and,*

In the discussion, the Commission notes that the change from listing contact information for a single operator to requiring the notice to list contact information for all operators will help parents find "…the appropriate party to whom to direct any inquiry". TRUSTe's opinion is that the listing of contact information for all operators will serve to confuse parents, and cause frustration (for example in the case where an operator's contact information is out-of-date or is unresponsive to a parent's inquiry). This will also require operators to constantly update their privacy notice as third party partnerships, relationships, or service providers change; thus making it a challenge for operators to maintain up-to-date accurate notices.

TRUSTe recommends the Commission maintain the current requirement around allowing a single operator to be designated as a point of contact in the case where there are multiple operators for a single website or online service. Note that such primary, or "first party" operator will have to retain responsibility for the notice and consent process for all "third party" operators "operating" under the first party operator's instruction.

The requirement of "…what information **each** operator collects…" will serve to continue to make notices onerous documents for parents to navigate, especially on a mobile device, as they try to figure out who each operator is and what it does with collected data. This does not meet the Commission's goal of streamlining the notice. As the Commission is aware, privacy notices are challenging to read as most privacy notices are typically written by someone with a legal background, and at a college reading level. A recent Law.com article by Paul Bond and Chris Cwalina notes:

> *The average adult in the United States reads at an eighth-grade level. Shannon Wheatman, Ph.D., a notice expert with Kinsella Media, LLC, recently reviewed the privacy policies of 97 Fortune 100 companies. (Three Fortune 100 companies have no privacy policies.) Wheatman found that on average, Fortune 100 companies drafted privacy policies at the reading level of a junior in college, well beyond general comprehension.*[5]

TRUSTe recommends § 312.4(b)(2) to be revised to read:

> *(2) A description of what information is collected from children through the website or online service, including whether the website or online service enables a child to make personal information publicly available; all uses of such information, and; the operator(s)' disclosure practices for such information*

[5] Paul Bond and Chris Cwalina, "Making Your Privacy Policy Comprehensive and Comprehensible," Corporate Counsel, 1 Sept. 2011, 18 Nov. 2011, http://www.law.com/jsp/cc/PubArticleCC.jsp?id=1202512963808.

Streamlining and simplifying notices can be done through how the notice is designed, as described further below.

Question 14: Should the Commission modify the notice requirement of the Rule to require that operators post a link to their online notice in any location where their mobile applications can be purchased or downloaded (e.g. in the descriptions of their application in Apple's App Store or in Google's Android Market)?

TRUSTe's Trusted Download Program requires its program participants to provide primary notice regarding what the software does (e.g. whether it tracks or will display ads), and access to other notices such as a privacy policy prior to the consumer consenting to installing the software.[6] A similar concept should be applied to mobile applications. Consumers should be able to make an informed decision on whether to install the mobile application including having access to the privacy policy.

TRUSTe supports adding the qualifier- "*any location where mobile applications can be purchased or otherwise downloaded*" - to the COPPA Rule notice requirement.

Question 15: Are there other effective ways of placing notice that should be included in the proposed revised Rule?

The proposed Rule changes will streamline the requirements for direct notices to parents, and recognize that relying on parents to comprehend a long privacy policy may not be the most effective way to get them the information they need to make an informed decision about their child's online activities. On November 30, 2011, TRUSTe released the results of its review of the privacy policies for the top Alexa 100 websites. We found on average privacy policies are 2462 words long and takes the average consumer about 10 minutes to read.[7] Simply put, consumers do not read privacy policies because they are too complicated and long.

TRUSTe has been exploring privacy policy design in order to make privacy policies easier for consumers to read by using simplified language and iconography to guide consumers. As part of that work, TRUSTe has developed a short notice design for both website and mobile privacy policies, boiling policies down to what consumers really want to know. These design concepts can be adapted to the direct notice and privacy policy requirements of the COPPA Rule.[8]

TRUSTe recommends the Commission require that the parental direct notice or the operator's privacy policy be optimized for the device it's displayed on. This can be done based upon screen size of the device so it is not platform specific, and should not place an undue burden on companies to support. Parents are then provided effective notice and can easily find the information they are looking for.

---

[6] TRUSTe, Program Requirements, 18 Nov. 2011, http://www.truste.com/pdf/Trusted_Download_Program_Requirements_Website.pdf.

[7] Devin Coldewey, " Examination of Privacy Policies Shows a Few Troubling Trends," TechCrunch, 30 Nov. 2011, 12 Dec. 2011, http://techcrunch.com/2011/11/30/examination-of-privacy-policies-shows-a-few-troubling-trends and similar finding at "Privacy Policy Infographic," Selectout Privacy Blog, 28 Jan. 2011, 18 Nov. 2011, http://selectout.org/blog/privacy-policy-infographic/.

[8] "Layered Policy Design," TRUSTe Blog, 20 May, 11 Nov. 2011, http://www.truste.com/blog/2011/05/20/layered-policy-and-short-notice-design/ and "Short Notice Privacy Disclosures," TRUSTe Blog, 23 May, 11 Nov. 2011, http://www.truste.com/blog/2011/05/23/short-notice-privacy-disclosures/.

TRUSTe would also like to see the Commission encourage innovation in improving how direct parental notices and privacy policies are presented in the same way the Commission is encouraging innovation around developing alternative forms of parental consent.

3. Parental Consent

Question 19: The Commission proposes eliminating the "email plus" mechanism of parental consent from § 312.5(b)(2). What are the costs and benefits to operators, parents, and children of eliminating this mechanism?

Email Plus is not an effective method for obtaining verifiable parental consent. The mechanism can be easily "gamed" by the child and is not effective in providing the parent direct notice regarding the operator's data collection practices. TRUSTe has long held this view and has never allowed Email Plus under its Children's Online Privacy certification program.[9] At a minimum, parental consent mechanisms should verify that the person providing consent is an adult. TRUSTe encourages taking consent mechanisms one step further by verifying the person providing consent is a parent or guardian authorized to provide consent.

Question 20: Proposed § 312.5(b)(3) would provide that operators subject to Commission-approved self-regulatory program guidelines may use a parental consent mechanism determined by such safe harbor program to meet the requirements of § 312.5(b)(1). Does proposed § 312.5(b)(3) provide a meaningful incentive for the development of new parental consent mechanisms?

TRUSTe encourages allowing safe harbor programs to approve parental consent mechanisms, as they will encourage innovation around alternative mechanisms or technologies for obtaining parental consent, while also improving the notice-consent experience for both child and parent.

One frustration that TRUSTe has observed among operators, is that current consent mechanisms require the child to leave the website or online service to go get the parent or stop using the website or online service until the parent checks their email to take additional steps. Clearly, there is opportunity here for operators to innovate around providing an improved experience.

It has been TRUSTe's experience that operators like to engage with the safe harbors early in the product development cycle. TRUSTe has worked with a number of operators - both start-ups and established businesses - and helped them review their parental consent mechanisms at different stages of the development cycle. It is a cost benefit to operators to engage early in having an outside party review the parental consent mechanism starting at either the design or wireframe stage.

4. Data Retention and Deletion

Question 22b. Should the Commission propose specific time frames for data retention and deletion?

In February 2011 TRUSTe updated its privacy certification program requirements with a specific provision requiring that clients state in their privacy policies how long they retain collected

[9] TRUSTe, "COPPA Program Requirements," 18 Nov. 2011, http://www.truste.com/pdf/Childrens_Privacy_Seal_Program_Requirements_Website.pdf.

data.[10] This program change generated questions from clients regarding how specific their privacy policies need to be regarding data retention.

Companies will face challenges complying with a specific timeframe requirement because the requirement could potentially conflict with other legal obligations such as statutes of limitation. A second challenge is the length of time of the relationship between child users and the operator may vary. For example, how long data is retained may depend on the child's continued engagement with the operator's website or online service. The operator may choose to deactivate a child's account or login due to a period of inactivity, or if a parent requests the operator to delete the child's information. Lastly, data retention policies may vary among business models depending on the type of data that is collected and the shelf life of that data. For example, links provided through social media outlets have a shelf life of only three hours.[11].

TRUSTe recommends the Commission not be too prescriptive in proposing data retention timeframes. Rather, we support having operators disclose what their data retention policies are in their privacy statements. In the alternative, TRUSTe recommends the Rule allow the privacy statement to disclose a retention period that is "…necessary to meet the [operator's] legal obligations. Also, guidelines in the COPPA FAQs would be more useful in this context rather than providing specific timeframes in the Rule itself.[12] In the past the Commission has used the COPPA FAQs to provide guidance regarding specific business use cases and these can be updated as new business use cases arise rather then making a change to the Rule itself.

5. Safe Harbors

Question 23: Proposed § 312.11(b)(2) would require safe harbor program applicants to conduct a comprehensive review of all member operators' information policies, practices, and representations at least annually. Is this proposed annual review requirement reasonable? Would it go far enough to strengthen program oversight of member operators?

While TRUSTe generally supports safe harbor audits, we feel that this particular requirement is unclear. Specifically, it is unclear whether this annual review is an evaluation of whether the operator has changed their practices (or not), or whether the review is a complete re-processing of the original certification of the operator's practices. TRUSTe uses certification coupled with ongoing monitoring to verify that an enrolled operator's privacy practices, consent mechanisms, and privacy policies have not changed since initial certification.

If a safe harbor is conducting ongoing monitoring throughout the annual certification period, then a complete re-certification of the operator's practices is not necessary as the safe harbor is aware of the operator's practices throughout the certification period. Annual re-certification, which includes reviewing the privacy policy, direct notice to parents, and the parental consent mechanism should verify that the operator's practices have not changed. Focusing on whether changes have been made since initial certification versus a full certification annually is much more scalable for the safe harbor to manage a growing program, so long as there is on-going monitoring as part of the safe harbor's processes.

---

[10] TRUSTe, Program Requirements, 18 Nov. 2011, http://www.truste.com/privacy-program-requirements/program-requirements.

[11] "You just shared a link. How long with people pay attention?'" Bitly Blog, 6 Sept. 2011, 18 Nov. 2011, http://blog.bitly.com/post/9887686919/you-just-shared-a-link-how-long-will-people-pay.

[12] "Frequently Asked Questions about the Children's Online Privacy Protection Rule," 7 Oct. 2008, 18 Nov. 2011, http://www.ftc.gov/privacy/coppafaqs.shtm.

Question 24: Proposed § 312.11(c)(1) would require safe harbor program applicants to include a detailed explanation of their business model, and the technological capabilities and mechanisms that will be used for initial and continuing assessment of member operators' fitness for membership in the safe harbor program. Is this proposed requirement reasonable? Would it provide the Commission with useful information about an applicant's ability to run a safe harbor program?

TRUSTe supports requiring safe harbor applicants to provide a detailed explanation of their business model, certification processes, and technical capabilities around administering a COPPA safe harbor program. It is important for self-regulatory programs to demonstrate impartiality, and show they use multiple methodologies (e.g. self-attestation, human review, and technology) to assess the level of an operator's compliance with the safe harbor's program standards. The approaches used to conduct certification, ongoing monitoring and re-certification needs to be balanced so the safe harbor is not heavily relying on any one methodology (e.g. self-attestation). Applicants should also include information regarding reporting that the safe harbor will provide enrolled operators regarding program compliance and frequency of that reporting.

Question 25a: Should the Commission consider requiring safe harbor programs to submit reports on a more frequent basis, e.g., annually?

TRUSTe supports requiring safe harbors to report on their programs annually. From a business standpoint, we believe that this requirement is more manageable and can be synced up with other annual reporting obligations. TRUSTe generates reports regarding program compliance for its U.S. – E.U. Safe Harbor Program on an annual basis and feels this would not be an unreasonable reporting frequency.

TRUSTe recommends annual reports be submitted within three months after the annual reporting period. For example for the reporting period Jan 1, 2012 – Dec 31, 2012 the report is submitted by March 31. 2013.

At this time, it is unclear which program metrics are to be reported to the Commission. Specifically, we think it's important to clarify whether COPPA reporting will include alleged program violations or focus on verified program violations. TRUSTe recommends that reporting be limited to uncured, verified program violations and aggregate metrics on the overall program rather than those pertaining to a specific operator. This preserves incentives for operators to stay within the COPPA safe harbor program.

Reporting on verified violations will provide the Commission more useful data regarding the safe harbor's effectiveness around managing its program. Requiring reporting of unverified and uncured violations by a specific operator will be a strong disincentive for any company to join a safe harbor program. The goal of reporting is to hold safe harbors accountable for properly administering their programs including demonstrating they are monitoring the practices of enrolled operators. This can be done without having to name the specific operator found in violation of the program. For example, reporting provided by the safe harbors could include:

- Total number of enrolled operators
    - Change from previous reporting period
- Total number of websites URLs or online services (e.g. mobile apps)
    - Change from previous reporting period

- Total number of program violations found and resolved
    - Total discovered through program monitoring
    - Total reported through a consumer feedback mechanism
- Breakdown by violation type and resolution (e.g. operator immediately corrected violation)
    - Failure to obtain parental consent prior to collecting personal information from a child
    - Personal information collection practices that do not fall under an allowable exception
    - Direct notice to parents missing required disclosures
    - Privacy policy missing required disclosures
    - Violation of certified privacy policy
    - Disclosure of a child's personal information to a third party without parental consent
    - Changed direct notice to parents or privacy policy without prior review by safe harbor
    - Materially changed practices without providing new notice and obtaining parental consent
    - Link to privacy policy not present
- Approval of alternative parental consent mechanisms
    - Outline what was approved and why it meets the requirements of the Rule

Question 25b: Should the Commission require that safe harbor programs report to the Commission a member's violations of program guidelines immediately upon their discovery by the safe harbor program?

As noted above, reporting requirements for the safe harbor programs need to balance two goals: providing the Commission assurances the safe harbors are monitoring the practices of their enrolled operators, while also giving operators incentive to join a COPPA safe harbor program. The annual report can include information on the types of program violations the safe harbor found during the reporting period and how these violations were handled.

It is not clear if the Commission is looking for immediate reporting on all verified program violations, or intentional violations where the operator has taken an action to violate the program. TRUSTe recommends the Commission limit required immediate reporting to intentional program violations. If all program violations are reported there will be a significant amount of "noise" the Commission will need to sift through to understand the data. The safe harbors are best equipped to make the determination if a violation is intentional versus a simple mistake.

The safe harbors need some flexibility to investigate and work with their certified operators to understand the scope of the violation (e.g. number of users affected), and work with operators to determine what needs to be corrected, the best approach for correcting the violation, and the timeframe in which to correct it.

To effectively investigate reported violations (e.g. through a consumer feedback mechanism) or discovered violations quickly, a safe harbor needs to engage with the operator upon discovery. Part of the process for reviewing reported violations is to replicate the consumer's reported experience. It may take time to replicate a reported violation through testing which would warrant deeper investigation. For example, when TRUSTe receives reports of sharing email

addresses with third parties without the consumer's consent, TRUSTe will perform email seeding to confirm there is a violation.[13]

Immediate reporting may not always be possible or prudent. In TRUSTe's experience, when program violations are found, its clients typically resolve found violations fairly quickly, at times in a matter of just a few days.

More importantly, immediate reporting by a safe harbor to the Commission of program violations could become a disincentive for companies to join a safe harbor program. There may be concerns by companies that reported violations would trigger further investigation by the Commission, and invite unwanted scrutiny that a company may not otherwise encounter, which is why TRUSTe recommends immediate reporting of only intentional program violations.

Reporting on a per incident basis may also hinder the safe harbor's investigative process by adding more steps to that process, and potentially impact the ability for the safe harbor to scale that process. By way of example - in 2010, TRUSTe received, reviewed, and processed over 7,700 consumer complaints. Out of those complaints, just 12% required the client to take action ranging from revising their privacy policy to changing data collection practices. TRUSTe uses the same process for investigating consumer complaints across all its certification programs so it is consistent (e.g. both clients and consumers know what to expect), and scalable (meaning the process can support an increase in volume as the number of TRUSTe certified companies grows).

TRUSTe appreciates the opportunity to provide comments on the proposed changes to the COPPA Rule and supports the overall direction of the Commission to provide continued privacy protections for children in light of emerging technologies.

TRUSTe hopes the Commission will consider the use cases and examples outlined above in thinking through the challenges and complexities around implementing the Rule changes as currently proposed.

For questions regarding these comments, please contact Joanne Furtsch, Director of Product Policy, at jfurtsch@truste.com.

Sincerely,

John P. Tomaszewski
General Counsel and Corporate Secretary

[13] [13] Email Seeding: TRUSTe creates multiple unique e-mail addresses and subscribes them via the client's site, using domain names and other information that do not in indicate a connection to TRUSTe. An alert is triggers if a seed address receives further e-mail after the unsubscribe request should have taken effect, helping to monitor on-going unsubscribe compliance.