SIIA POLICY

March 11, 2024

Ms. April Tabor
Secretary
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Suite CC-5610 (Annex E)
Washington, D.C. 20580

**re: COPPA Rule Review, Project No. P195404**

Dear Ms. Tabor,

On behalf of the Software & Information Industry Association ("SIIA"), we write in response to the Federal Trade Commission's ("Commission") request for comment on the Commission's notice of proposed rulemaking ("NPRM") on Children's Online Privacy Protection ("COPPA") Rule ("Rule"). We appreciate the Commission's attention and diligence to the release of ongoing guidance and look forward to working with the commissioners and staff as this process moves forward.

SIIA understands the importance of the Commission's oversight role and appreciates the opportunity to respond to the NPRM. On behalf of the members of our association, we submit to the Commission to review our comments pertaining to the following themes:

- The role of education technology ("ed tech") and the impact of the Rule on vendors.
- The collaboration between the Commission and the Department of Education ("ED") in establishing rules that continue to promote student success in learning.
- The advancement of technologies and the Rule's impact on innovation practices.
- The role of accessibility of technology and the Rule's effect on digital equity.
- The safety of children and promotion of parental control in and outside of the classroom.

SIIA is the principal trade association for companies in the business of information. Our members include nearly 375 companies reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms

used by millions worldwide, and companies specializing in data analytics and information services. Our ed tech members partner with educational agencies and institutions to provide innovative digital tools for learning, school administration, academic assessment, and more. In addition, all of our nation's schools collaborate and depend on our ed tech members to assist learners in learning how to thrive in a skilled workforce.

We are pleased the Commission has taken steps to finish the COPPA rulemaking process begun in 2019. In response to the original Request for Comment ("RFC"), SIIA submitted a detailed response to address what we believed would make the Rule more sustainable and consistent with the current technology landscape. SIIA thanks the Commission for considering and explicitly acknowledging our 2019 comments.

As the Commission is aware, ed tech is not new. Technology has been used in schools for decades. The overnight switch to virtual learning in 2020 put a focus on the use of educational technology around the globe. This transition both demonstrated the critical role of ed tech in schools and student learning and highlighted the importance of digital equity and equitable access to these technologies.

The Commission has been active in ensuring operators work within the guardrails of the existing Rule. The 2022 policy statement on ed tech[1] clearly outlined the expectations of the Commission. We released a statement thanking the Commission for this action.[2] Additionally, the May 2023 Edmodo lawsuit was a clear example of the Commission exercising its authority under the existing Rule in a meaningful way.[3] This lawsuit provided ed tech companies with additional guidance on how operators should implement COPPA when working on behalf of schools.

The proposed Rule takes many steps to clarify important aspects of the law that have been unclear for decades, including how COPPA works in the schools. We also appreciate the efforts to update the Rule to keep it current in light of current technologies. Our responses to the changes outlined and specific questions in the NPRM follow.

General Questions

---

[1] https://www.ftc.gov/system/files/ftc_gov/pdf/Policy%20Statement%20of%20the%20Federal%20Trade%20Commission%20on%20Education%20Technology.pdf

[2] https://www.siia.net/siia-statement-on-todays-ftc-vote-on-coppa/

[3] https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ed-tech-provider-edmodo-unlawfully-used-childrens-personal-information-advertising

**1. Please provide comment on any or all of the provisions in the proposed Rule. For each provision commented on, please describe: (1) the impact of the provision(s) (including any benefits and costs), if any; and (2) what alternatives, if any, the Commission should consider, as well as the costs and benefits of those alternatives.**

**Comments on "Actual Knowledge" Standard**

We agree with the Commission's decision to align to the existing statutory authority and maintain the actual knowledge standard. Maintaining the existing knowledge standard ensures clarity in the Rule going forward and does not go beyond the Commission's authority.

Congress originally adopted the standard for "knowingly" to include "actual, implied and constructive" in its definition. However, in the final legislation, Congress decided to keep the standard as "actual knowledge" after hearing expert testimony. Having a "constructive knowledge" standard will create more confusion and uncertainty for operators. We concur with the intent set by Congress and support the Commission on declining to change the standard to "constructive knowledge."

**Comments on Proposed Definitions in § 312.2**

We believe it is appropriate to modify the definitions to the Rule to keep pace with current technologies and practices. This allows the Rule to maintain relevance without the need to do reauthorizations of the law with every change of technology or practice. Our responses to select proposals follow:

*Online Contact Information*

- Proposed Modification: The Commission proposes amending the definition of "online contact information," by adding "mobile telephone number" as an identifier, provided the operator uses only to send a text message'' to the non-exhaustive list of identifiers that constitute ''online contact information.''
    - SIIA Response: We agree and support the Commission's addition of "mobile telephone number" as an identifier of online contact information. We believe that this addition is reflective of the current technology landscape.

*Personal Information*

- Proposed Modification: The Commission proposes to expand the definition of "personal information" by adding "*biometric data*" as a proposed modification to ensure that the Rule keeps pace with the advancement of technology by using biometrics as a means of identification.

- SIIA Response: We do not agree with the inclusion of a biometric identifier to the definition of "personal information" as it exceeds the FTC statutory authority and creates inconsistencies with state privacy laws and FTC guidance.

  The COPPA statute is explicit that the FTC only has the authority to add identifiers to the definition of personal information that "permit the physical or online contacting of a specific individual." It is not enough under the statute that the identifier can be used to recognize an individual. Rather, the identifier must permit physical or online contacting of a specific individual. The FTC has not demonstrated this high standard is met with respect to the various elements included in the proposed biometric identifier definition.

  We also request clarification as to the meaning of "data derived from voice data" in the addition of biometric data to the definition of "personal information". Certain technology-based literacy products may include features for students to record themselves reading, for purposes of phoneme-level assessments of decoding skills and giving students an opportunity to practice and improve their reading. "Data derived" from these recordings may include skills assessment, time spent, and other usage information, including correlations among these secondary data sets. It is our members' view that this type of data, when not identified or identifiable with a child, should not be considered personal information under COPPA. That may be the intent behind the definition; if so, we request that this be made explicit, such as by changing a "biometric identifier that can be used" to a "biometric identifier that is used" at the beginning of the new clause (10) of the definition.

  Additionally, biometric data may be collected and promptly deleted to comply with other state, federal, and international laws and regulations. If the biometric data is collected and promptly deleted it should not fall within the scope of the COPPA consent requirements.

- Proposed Modification: The Commission inquires about expanding the definition of "personal information" by adding *avatars* generated from a child's image as a means of identification.
  - SIIA Response: We do not agree with including avatars in the definition of "personal information" unless the avatar permits the physical or online contacting of a specific individual.

The FTC lacks a statutory basis for including avatars in the Rule's definition of personal information. As discussed, the statute permits the FTC to expand the definition of "personal information" only where the information, on its own, is "individually identifiable" and "permits the physical or online contacting of a specific individual." There is no demonstration that an avatar generated from an image satisfies either requirement. To the contrary, operators utilize such avatars, similar to anonymous user and screen names, to allow a user to personalize their settings and experiences (such as game leaderboards and filtered or moderated chat) without collecting identifiable information.

*School/School Authorized Education Purpose*

- Proposed Modification: The Commission, in order to codify current guidance,[4] proposes adding definitions for "school" and "school authorized education purpose" to align to the proposed exception for parental consent.
    - SIIA Response: We support adding "school" and "school authorized education purpose" to the existing definitions in the Rule. These additions will provide much needed clarity on how an operator can partner with a school to meet the needs of its educational community. Our full response to these definitions are below.

*Internal Operations*

- Proposed Modification: The Commission proposes to keep the definitional language that covers such the enumerated activities that are necessary to "maintain or analyze the functions'' of the website or service.
    - SIIA Response: We support maintaining the enumerated activities listed in the Rule.
- Proposed Modification: The Commission plans to prohibit operators from contacting an individual, in order to ''[f]ulfill a request" - and wants to strike the exception from using or disclosing personal information in connection with processes, including machine learning processes, that encourage or prompt use of a website or online service.
    - SIIA Response: We are concerned about removing this exception for use restrictions. In particular, when it comes to machine learning "prompting" or "nudging," there are circumstances where these features may be used for the benefit of the consumer. For example, a company

4 https://www.ftc.gov/system/files/ftc_gov/pdf/Policy%20Statement%20of%20the%20Federal%20Trade%20Commission%20on%20Education%20Technology.pdf

may employ the technology to encourage privacy-aware behaviors or to take a break from using the service.

Additionally, algorithmic or machine learning prompts for the purposes of meeting learning objectives should be allowed in the context of education technology (specifically adaptive and/or personalized learning).

The current Rule strikes the right balance allowing operators to collect persistent identifiers to serve contextual advertising without providing notice or obtaining parental consent. Contextual advertising is critical to maintaining free high-quality content for children and is different from targeted advertising.

*Website or Online Service Directed to Children*

- Proposed Modifications: The Commission believes that the Rule's multi-factor test, which applies a "totality of the circumstances" standard, is the most practical and effective means for determining whether a website or online service is directed to children.
    - SIIA Response: We support the "totality of the circumstances" test as the most effective means to determine if a website or online service is directed to children.

- Proposed Modification: The Commission proposes adding examples of specific evidence to identify audience makeup including reviews by users or third parties, similar websites or online services, and the age of users on similar websites or online services.
    - SIIA Response: We do not think the Rule should be expanded to include reviews by users or third parties, similar websites or online services, and the age of users on similar sites and services as examples. These examples are outside of a business's direct control and may not appropriately represent the intent or actual activities of the business. Determining whether websites or services are "similar" is highly subjective, as are reviews by users or third parties. Thus, adding these additional examples will create uncertainty for businesses as to whether their websites or services will be considered child-directed.

**Comments on Proposed Changes to Notice Provisions in § 312.4**

*Direct Notice to the Parents*

- Proposed Modification: The Commission proposes adding references to ''school'' in the Rule to cover the situation in which an operator relies on authorization from a school to collect information from a child and provides direct notice to the school rather than to the child's parent.
    - SIIA Response: We support the Commission's proposal of adding "school" when an operator relies on authorization from a school to collect information from children. We agree that an operator should make reasonable efforts to ensure the school receives the direct notice. This could take place during the contracting process or as part of the online sign up process.

      This may also be an area where additional joint guidance from the Commission and ED is warranted. This guidance could focus on best practices for providing direct notice, how schools can review the direct notice, and how to align this with the Family Education Rights and Privacy Act (FPERA) requirements of a school official.[5]

- Proposed Modification: The Commission also proposes to require that operators sharing personal information with third parties identify the third parties or the categories of third parties as well as the purposes for such sharing, should the parent provide consent.
    - SIIA Response: We suggest clarifying that an operator is not prohibited from linking from the direct notice to a separate disclosure page that lists all of the required information.

**Comments on Proposed Changes to Parental Consent Provisions in § 312.5**

*Parental Consent*

- Proposed Modification: The Commission is seeking comment on whether parental consent is needed if an operator institutes a feature that prompts or enables a child to communicate with a chatbot or other similar computer program that simulates conversation, that operator must first collect verifiable parental consent.
    - SIIA Response: We believe that simply placing a chatbox within an online platform should not trigger the requirement to obtain consent from a parent. Chatbots, for example, can be used for things like

[5] 34 C.F.R. 99.31

tutoring and have a broad base of research supporting the efficacy of the tool.

We do support requiring parental consent if the chatbot is used on a site directed to children and is designed to request personal information.

- Proposed Modification: The Commission welcomed the development of methods that prove less cumbersome for operators while still meeting COPPA's statutory requirements, specifically related to the verifiable parental consent requirements for operators
    - SIIA Response: We agree with the Commission's mentioning of "general concerns" that COPPA's consent methods create "friction," as it seems duplicative and could create "consent fatigue." We are opposed to the requirements to collect a separate consent for disclosures to third parties. We suggest allowing check boxes or similar features to streamline or consolidate consent instead of duplicating a process that may lead to more consent fatigue.

- Proposed Modification: The Commission welcomes further information on the role that platforms could play in facilitating the obtaining of parental consent.

    - SIIA Response: We do not support the requirement of platform-based consent. For example, vendors in the education space cannot shift COPPA obligations to a school, so similarly, vendors should not be able to shift COPPA obligations to a platform.

- Proposed Modification: The Commission also proposes adding two parental consent methods to § 312.5(b) including one based on facial recognition.
    - SIIA Response: We are concerned that the Commission's proposal to add biometric requirements necessitates the disproportionate collection and processing of personal information to access a service. It would also create an undue burden on parents that wish to allow children to access online services by requiring parents to not only provide a government ID but also to go through a facial recognition process. Requiring human comparison is likely less accurate and more burdensome than automated comparison, and effectively erases any efficiencies operators would gain from using automated facial recognition technology. This proposal introduces more friction into user experiences and disincentivizes parents from allowing children to

engage with otherwise age appropriate content. The Commission should remove the requirement that the two images be reviewed by a human given the burden and the lower accuracy.

*School Authorization Exception*

- Proposed Modification: The Commission proposes codifying in the Rule its long-standing guidance that schools, State educational agencies, and local educational agencies may provide consent *in loco parentis* for the collection of personal information from students younger than 13 in limited circumstances; specifically, where the data is used for a school-authorized education purpose and no other commercial purpose.
    - SIIA Response: Our members support the Commission and their efforts to emphasize and clarify the longstanding guidance for the education community. We support this codification, as our members have come to rely on the COPPA FAQ and the ed tech guidance policy statement as important pillars for how companies should protect the privacy and security of personal information collected from children in a school setting.

      We are pleased the Commission recognizes the difficulty in "obtaining consent from the parents of every student in a class often will be challenging, in many cases for reasons unrelated to privacy concerns." By giving schools the ability to provide consent, the Commission is both easing the administrative burden for school staff and minimizing the amount of unnecessary data a vendor may need to collect. Most vendors in a school setting do not have direct relationships with parents. Parents have traditionally exercised FERPA rights to access data through the school and should do the same under COPPA. This is another area where the Commission and ED may consider curating joint guidance together.

      We also support requiring a written contract and agreement between the ed tech provider and the school, which provides the expectations and requirements of consent, limitations/usage of data, and disclosure. We would appreciate clarification that a "click-wrap agreement", so long as it meets all of the necessary privacy, security, notice and disclosure requirements under COPPA, would also be considered a written agreement.[6] This written agreement aligns with the FERPA rules

[6] ED's 2014 guidance, "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices," outlines "click-wrap" agreements on page 8 as "the act of clicking a button to accept the TOS serves to enter the provider and the end-user (in this case, the school or district) into a contractual relationship akin to

and builds upon the protections that FERPA provides when accessing student data.

We also suggest allowing for flexibility on whether the "written agreement" requirement is at the level of the state, consortium, district or school level, as our members' experience is that the data privacy agreements presented to them by educational customers are rarely done at the school level. Limiting these agreements to the school level, when in reality the district or other higher level administrative entity may have the requisite authority, risks significantly burdening school personnel and burdening the contracting process, thus restricting or slowing students' access to educationally beneficial technology.

We urge the Commission to emphasize flexibility around the definition of "school-authorized education purpose." Schools in the United States make decisions locally and may have different approaches to how they want to use the data they authorize an operator to collect on their behalf. For example, a school district may want to find a vendor that can help them build out a math curriculum for 6th, 7th, and 8th grade students. This may include a suite of products focused on a variety of math skills and the school requests the vendor help them analyze student longitudinal development. Another school may want to have distinct math products from different vendors but also have those products "talk" with each other so they can track student mastery of skills across the curriculum and identify areas where the student might need extra support.

We also urge the Commission to reconsider the requirement that the written agreement between the operator and the school indicate the name and title of the person providing authorization on behalf of the school (proposed Sec. 312.5(c)(10)), for several reasons. First, data protection agreements and similar documents entered into by operators with educational agencies may be done at the state level, consortium level, district level or school level. Requiring school-level information in a state-wide or other higher-level agreement will slow down the contracting process. Second, our members report that many of their education customers have staff turnover and that keeping current and accurate contact information for them is an ongoing challenge. Third, the exception does not indicate what the practical effect is of this requirement. Our members are concerned that this

signing a contract." https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf

requirement could be interpreted by schools to mean that the named individual must take all actions or sign off on all documentation in relation to providing student data to the operator, which would present a new operational challenge in the provision of digital products and services to schools. In our members' experience, educational agencies are typically careful to ensure that the persons who sign legal documentation are properly authorized, and feel that this level of contracting detail is best left up to the educational institutions.

- Proposed Modifications: The NPRM proposes to add to the definition of "school-authorized education purpose" by including product improvement and development (as well as other uses related to the operation of the product, including maintaining, supporting, or diagnosing the service), provided the use is directly related to the service the school authorized. It intends to permit operators to improve the services of the technology.
    - SIIA Response: We agree with adding "product improvement and development" to the definition of school-authorized education purpose. Data is a critical tool in the education space helping students, educators, and parents understand where a student is on their educational journey and how best to support that student. Continuous innovations in ed tech tools allow for students to master skills at their own pace, get extra help outside of school, and find educational tools that can supercharge their educational journey.

      Operators must be able to improve their products to respond to the needs of their vendors. The Commission has requested specific examples of how operators may use data for "product improvement and development." We urge flexibility but are providing a non-exhaustive list of how vendors may use data to improve their

      Additionally, we advocate for clarification of the meaning of "directly related to the service the school authorized". Operators who learn about a deficiency in student skills in a particular area may be able to use that information to develop an additional product or service to address that need. Generally, this can be done without personal information, however, in the rare instances where personal information is better suited for this purpose, its use should be permitted provided that all other COPPA safeguards are observed.

- Proposed Modifications: The Commission proposes the need for "flexibility" when it comes to the question on who should be able to provide authorization for data collection under this exception.

- SIIA Response: We agree with a flexible approach, as many states and districts operate with different procedures.

- Proposed Modification: The Commission proposes adding a paragraph to give schools the right to review personal information collected from a child, as well as refuse to permit operators' further use or future online collection of personal information, and to direct operators to delete such information.
    - SIIA Response: We agree with the addition of this paragraph, as it ensures that schools maintain direct control of the data provided by the technology, which aligns with FERPA's school official exception.

- Proposed Modification: The NPRM proposes to add additional clarity to the Confidentiality, Data Security and PI collected from children, by splitting the operator's requirements into discrete paragraphs and providing further guidance as to steps operators can take to comply with each requirement. Specifically, the paragraphs will mention "reasonable procedures" that must be established to protect confidentiality and security, as well as the "reasonable steps" required for the operator to take when releasing children's PI.
    - SIIA Response: We support the additional security measures that are recommended in the Rule, as the security and confidentiality of children's PI are essential to the intent of the Rule. We urge clarification from the Commission that a vendor can meet the new data security requirements as part of an already established, broader security program, instead of requiring the creation of a new, additional, duplicative security program solely focused on children.

- Proposed Modifications: The Commission proposes to be more explicit in the duties of the operator's requirements for data retention and deletion, by adding the mandate of having a written policy, specifying its business need for retaining children's personal information and its timeframe for deleting it, precluding indefinite retention.
    - SIIA Response: We support this measure of the Commission to require a written policy on how children's data may be used, retained, and deleted.

      In a school setting, the school should determine the retention and deletion schedule. In many instances,the data collected by operators on behalf of a school are used for state and federal reporting purposes and may be subject to separate state and federal education laws.

**Comments on Proposed Changes to Data Retention and Deletion Requirements in § 312.10**

- Proposed Modifications: The Commission proposes to limit the circumstances under which an operator may retain personal information, instead of permitting retention "for specified, necessary business needs," the proposed Rule would permit retention only "to fulfill the specific purpose(s) for which the information was collected and not for a secondary purpose." The proposed Rule would not permit operators to retain data indefinitely. The Commission proposes these changes in part to further the goal of data minimization.
    - SIIA Response: We support measures to minimize data collection and retention[7]. We request the Commission provide exceptions for secondary purposes that are essential to the safety and security of online platforms and children. Specifically, we recommend the Commission clarify exceptions necessary for security, fraud & abuse prevention, financial record-keeping, complying with legal or regulatory requirements, ensuring service continuity, or ensuring the safety and age appropriateness of the service.

Definitions

**2. As part of the Rule review that led to the 2013 Amendments, the Commission determined that an operator will not be deemed to have "collected" (as that term is defined in the Rule) personal information from a child when it employs technologies reasonably designed to delete all or virtually all personal information input by children before making information publicly available. The Commission is concerned that, if automatic moderation or filtering technologies can be circumvented, reliance on such technologies may not be appropriate in a context where a child is communicating one to one with another person privately, as opposed to posting information online publicly. Should the Commission retain its position that an operator will not be deemed to have "collected" personal information, and therefore does not have to comply with the Rule's requirements, if it employs automated means to delete all or virtually all personal information from one-to-one communications?**

We support retaining the 2013 amendments especially given the privacy-protective provision to use an automated means to delete all or virtually all personal information.

[7] https://www.siia.net/siia-child-and-teen-privacy-and-safety-principles/

**3. The Commission proposes to include mobile telephone numbers within the definition of "online contact information" so long as such information is used only to send text messages. This proposed modification would permit operators to send text messages to parents to initiate obtaining verifiable parental consent. Does allowing operators to contact parents through a text message to obtain verifiable parental consent present security risks to the recipient of the text message, particularly if the parent would need to click on a link provided in the text message?**

We support the proposal to amend the Rule's definition of "online contact information" to include "an identifier such as a mobile telephone number provided the operator uses it only to send a text message." The rationale for permitting this practice, which is currently prohibited, is not collection but advances in technology. For example, mobile telephone numbers are frequently used to obtain verifiable parental consent (VPC). This is distinct from collecting consumer data for advertising or similar purposes, and the data cannot be used for such purposes anyway with the proposed language. Moreover, mobile text is frequently the most efficient compliance tool.

Furthermore, additional security risk is minimal, especially if VPC is conducted via a website. There are, of course, examples of mobile numbers being misused for fraudulent purposes. For example, texts may be sent falsely claiming packages have been delivered and requesting fraudulent "handling" or associated fees. However, this risk can be ameliorated by text requests that direct the user to a secure site or login page. In this way, any inherent reduction in security due to mobile numbers can be avoided. They would simply permit VPC in situations where a parent's intent is not otherwise verifiable, broadening children's access in contexts otherwise compliant with COPPA.

**5. The Commission proposes adding biometric identifiers such as fingerprints, retina and iris patterns, a DNA sequence, and data derived from voice data, gait data, or facial data to the definition of "personal information." Should the Commission consider including any additional biometric identifier examples to this definition? Are there exceptions to the Rule's requirements that the Commission should consider applying to biometric data, such as exceptions for biometric data that has been promptly deleted?**

We do not agree with the inclusion of a biometric identifier in the definition of "personal information" as it exceeds the FTC statutory authority and creates inconsistencies with state privacy laws and FTC guidance.

The COPPA statute is explicit that the FTC only has the authority to add identifiers to the definition of personal information that "permit" the physical or online

contacting of a specific individual." It is not enough under the statute that the identifier can be used to recognize an individual. Rather, the identifier must permit physical or online contacting of a specific individual. The FTC has not demonstrated this high standard is met with respect to the various elements included in the proposed biometric identifier definition.

However, we encourage the Commission to specifically exempt data that is promptly deleted when used as a compliance tool. Biometric data collection typically occurs in two contexts: long-term data collection and analysis, and incidental collection for the purposes of fraud and abuse prevention, complying with legal or regulatory requirements, service continuity, and ensuring the safety and age-appropriateness of the service. Biometric data that is promptly deleted falls almost exclusively into this latter category.

**6. The use of avatars generated from a child's image has become popular in online services, such as video games. Should an avatar generated from a child's image constitute "personal information" under the COPPA Rule even if the photograph of the child is not itself uploaded to the site or service and no other personal information is collected from the child? If so, are these avatars sufficiently covered under the current COPPA Rule, or are further modifications to the definition required to cover avatars generated from a child's image?**

We disagree. Avatars do not constitute "individually identifiable information about an individual," as the statutory definition of "personal information" requires. Additionally, if the image of the child in question does not leave the device, no personal information is "collected" under COPPA. Furthermore, allowing users to create avatars generated from an image is a privacy-protective alternative that should be encouraged, consistent with data minimization principles and FTC guidance encouraging blurring or other modifications to a child's image before it is publicly displayed.

The FTC lacks a statutory basis for including avatars in the Rule's definition of personal information. As discussed, the statute permits the FTC to expand the definition of "personal information" only where the information, on its own, is "individually identifiable" and "permits the physical or online contacting of a specific individual." There is no demonstration that an avatar generated from an image satisfies either requirement.

**8. The definition of "personal information" includes "information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in [the Rule's definition of `personal information']." Does the phrase "concerning the child or parents of that child" require further clarification?**

We believe this phrase requires clarification regarding how attenuated the data must be from the "child or parents of that child." The word "concerning" is a vague and potentially overbroad term. For example, information concerning a child of their parents could be as attenuated from their identity as general demographic data that describes that household. Instead, we suggest best practices found within US privacy law. This language defines the data set more clearly as "linked or reasonably linkable to" the child or parents of that child.

**9. Certain commenters recommended modifications to the "support for the internal operations of the website or online service" definition, including to limit personalization to "user-driven" actions and to exclude methods designed to maximize user engagement. Under what circumstances would personalization be considered "user-driven" versus personalization driven by an operator? How do operators use persistent identifiers, as defined by the COPPA Rule, to maximize user engagement with a website or online service?**

We support the Commission's acknowledgment that the definition of "internal operations" already covers user-driven and user-engagement personalization, as well as enhanced personalization techniques based on operator-driven first-party metrics and inferences. However, the Commission's proposal to prohibit operators from using this exception to "optimize user attention or maximize children's engagement" —highlighting using notifications or prompts to drive such engagement—without verifiable parental consent is unclear and could have unintended consequences if defined too broadly.

Specifically, this proposal, applied to prompts and notifications, could create less transparency and control for children. For example, it could prohibit notifications about location tracking in the absence of VPC. As such, it is important for the Commission to differentiate between techniques used solely to promote a child's engagement and techniques that provide other functions, such as personalizing a child's experience. This issue could be solved with a narrow interpretation regarding prompts or notifications such that only prompts or notifications that have a commercial aspect (e.g., push notifications promoting purchases or targeted advertising), or that facilitate or enable access to interactions with third parties would require VPC.

Furthermore, the Commission would require businesses that use the "internal operations" exception to disclose those internal operation cases. While we understand and agree with the policy goal, the Rule as written is overbroad. As an initial matter, such disclosures would not be fundamentally useful for a parent because most internal uses are technical, such as for improving the service. Second, the Rule risks compromising competitive or otherwise sensitive business information. For example, an important activity covered by the internal operations exception is

"the security or integrity of the user, website, or online service," and it is unclear whether the Commission would require operators to reveal previously undisclosed and potentially sensitive security practices. Those who seek to exploit vulnerabilities within an operator's service may be able to leverage such disclosures found within their notices to compromise websites, services, or their users.

Instead, the Commission should require the disclosure of clear, concise and accurate information necessary for parents to provide meaningful informed consent. Such disclosures should clearly state that the regulation does not require the disclosure of sensitive business information that could compromise the safety, security, or competitiveness of the operator.

**10. Operators can collect persistent identifiers for contextual advertising purposes without parental consent so long as they do not also collect other personal information. Given the sophistication of contextual advertising today, including that personal information collected from users may be used to enable companies to target even contextual advertising to some extent, should the Commission consider changes to the Rule's treatment of contextual advertising?**

This issue could be solved with a narrow interpretation regarding prompts or notifications such that only prompts or notifications that have a commercial aspect (e.g., push notifications promoting purchases or targeted advertising), or that facilitate or enable access to interactions with third parties would require VPC.

The current Rule strikes the right balance allowing operators to collect persistent identifiers to serve contextual advertising without providing notice or obtaining parental consent. Contextual advertising is critical to maintaining free high-quality content for children.

**11. With regard to the definition of "website or online service directed to children," the Commission would like to obtain additional comment on whether it should provide an exemption for operators from being deemed a child-directed website or online service if such operators undertake an analysis of their audience composition and determine no more than a specific percentage of its users are likely to be children under 13.**

We believe that the Commission properly determined that under current law it cannot incorporate a constructive knowledge standard or cover sites or services "likely to attract" children under the age of 13. Although the NPRM attempts to clarify when a service is "directed to children" by providing specific examples that demonstrate the intended or actual audience of operators, the proposal instead introduces new factors that are not directly tied to the activities or intention of the business. These include references to third parties, similar websites, and the age of users on the site. We do not believe these are necessary nor sufficient to predict the

likelihood of attracting children. Furthermore, such attempts at a constructive knowledge standard are in any case unnecessary and counterproductive, and would only serve to cloud well-intentioned compliance efforts.

Notice

**12. The Commission proposes requiring operators that share personal information with third parties to identify those third parties or specific categories of those third parties in the direct notice to the parent. Is this information better positioned in the direct notice required under § 312.4(c), or should it be placed in the online notice required under § 312.4(d)?**

We believe this is best placed in the online notice and linked to from the direct notice.

Parental Consent

**13. Can platforms play a role in establishing consent mechanisms to enable app developers or other websites or online services to obtain verifiable parental consent? If so, what benefits would a platform-based common consent mechanism offer operators and parents? What steps can the Commission take to encourage the development of platform-based consent mechanisms?**

We do not believe that platforms should have an obligation to develop a VPC method for third party developers and their services. It is important for the Commission to reiterate that the implementation duties remain on the developer, such that the developer—not the platform—is responsible for limiting app privileges to comply with the consents that parents provide.

**14. To effectuate § 312.5(a)(2), which requires operators to give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of the child's personal information to third parties, the Commission proposes requiring operators to obtain separate verifiable parental consent prior to disclosing a child's personal information, unless such disclosure is integral to the nature of the website or online service. Should the Commission implement such a requirement? Should the consent mechanism for disclosure be offered at a different time and/or place than the mechanism for the underlying collection and use? Is the exception for disclosures that are integral to the nature of the website or online service clear, or should the Commission clarify which disclosures are integral? Should the Rule require operators to state which disclosures are integral to the nature of website or online service?**

We support incorporating the consent mechanism for third-parties disclosures into the broader first-party VPC process for the collection and use of personal information. This prevents requiring VPC to be obtained twice. However, capturing VPC this way is only workable if the Commission allows for reasonable implementation procedures. For example, operators should be able to use a clear disclosure and check box acknowledgment to capture VPC for disclosures to third parties as part of their own VPC for first-party collection and use. This would streamline consent instead of duplicating a process and risking notice fatigue.

Furthermore, requiring the disclosure of business practices necessary to ensure compliance with a law would again likely expose sensitive, nonpublic business information. Describing how an operator will avoid certain data processing would also likely be unhelpful to the average parent looking to understand how the business plans to collect and use the data of their child using the service.

**15. As noted in Part IV.C.3.c., the Commission proposes to modify § 312.5(c)(4) to prohibit operators from utilizing this exception to encourage or prompt use of a website or online service. Are there other engagement techniques the Rule should address? If so, what section of the Rule should address them? What types of personal information do operators use when utilizing engagement techniques? Additionally, should the Rule differentiate between techniques used solely to promote a child's engagement with the website or online service and those techniques that provide other functions, such as to personalize the child's experience on the website or online service? If so, how should the Rule differentiate between those techniques?**

When it comes to "prompting" or "nudging," there are circumstances where these features may be used for the benefit of the consumer. For example, a company may employ the technology to encourage privacy-aware behaviors or to remind the user to take a break from using the service. Additionally, some operators may use nudge or prompt techniques to encourage a user to seek out help or assistance.

Additionally, algorithmic or machine learning prompts may be used to remind a student to turn in homework assignments, a parent to sign a permission slip, or for a teacher to submit attendance for the day. Special consideration must be given to the use cases whether in school or out of school and we caution against broad language that may unintentionally restrict the use of useful reminders.

**16. The Commission proposes to include a parental consent exception to permit schools, State educational agencies, and local educational agencies to authorize the collection, use, and disclosure of personal information from students younger than 13 where the data is used for a school-authorized education purpose and no**

**other commercial purpose. What types of services should be covered under a "school-authorized education purpose"? For example, should this include services used to conduct activities not directly related to teaching, such as services used to ensure the safety of students or schools?**

We urge the Commission to emphasize flexibility around the definition of "school-authorized education purpose." Schools in the United States make decisions locally and may have different approaches to how they want to use the data they authorize an operator to collect on their behalf. For example, a school district may want to find a vendor that can help them build out a math curriculum for 6, 7, and 8th grade students. This may include a suite of products focused on a variety of math skills and the school requests the vendor help them analyze student longitudinal development. Another school may want to have distinct math products from different vendors but also have those products "talk" with each other so they can track student mastery of skills across the curriculum and identify areas where the student might need extra supports. We urge caution against the Commission being too prescriptive on activities here because it is not an expert in how each school addresses community needs. Broad flexibility and engagement with ED to provide implementable and clear guidance will protect the privacy of students and will not lead to unnecessary overreach.

Thank you for your time and consideration of our comments on this NPRM. We look forward to continuing to engage with the Commission during this process and in other initiatives to advance children's online privacy and safety. Please send any questions to SIIA's Vice President for Education and Children's Policy, Sara Kloek, at skloek@siia.net.

Respectfully submitted,

Sara Kloek
VP, Education and Children's Policy
Software & Information Industry Association