Software & Information Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095

December 23, 2011

The Honorable Donald S. Clark
Secretary
Federal Trade Commission
Room H-113 (Annex E)
600 Pennsylvania A venue
NW Washington, DC 20580

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

Dear Secretary Clark,

The Software & Information Industry Association (SIIA) appreciates the opportunity to comment on the Federal Trade Commission's ("FTC" or "Commission") proposal to amend the Children's Online Privacy Protection Rule ("COPPA Rule" or "Rule"), 16 CFR part 312, issued pursuant to the Children's Online Privacy Protection Act (COPPA).

As the principal trade association of the software and digital information industry, the more than 500 members of SIIA develop and market software and electronic content for business, education and consumers. SIIA's members are software companies, e-businesses, and information service companies, as well as many electronic commerce companies. As leaders in the global market for innovative software and information products and services, our membership consists of some of the largest and oldest technology enterprises in the world, as well as many smaller and newer companies. For nearly two decades, SIIA has worked with policymakers at the Federal and state levels in the United States, and around the world, to examine the implications and operations of privacy and related laws.

I. General Comments, Application of the COPPA Rule

Congress enacted the Children's Online Privacy Protection Act of 1998[1] to prohibit unfair or deceptive acts or practices in connection with the collection, use, or disclosure of personally identifiable information from children on the Internet. SIIA shares the Commission's commitment to helping maintain a safe, secure online experience for children and to ensure that COPPA continues to meet its originally stated goals, even as technologies change. To that end, SIIA appreciates and supports the Commission's effort to review and make certain modifications to the Rule in order to respond to changes in Internet technology and user behavior.

[1] 15 U.S.C. 6501

Tel: +1.202.289.7442
Fax: +1.202.289.7097
www.siia.net

SIIA supports many of the Commission's conclusions put forth in the Notice of Proposed Rule, while recommending modifications and additions in other cases. These are articulated below. First, with respect to application of the Rule, SIIA supports the Commission's following key conclusions.

A. COPPA's Definition of a "Child"

SIIA supports the FTC's conclusion not to seek expansion of the Rule to "an individual under the age of 13." SIIA agrees with the Commission that it would not be effective or appropriate to extend COPPA's application to adolescents. SIIA believes that recent and future technological developments will continue to provide additional tools to enhance privacy and improve the processes for notice and consent about the potential collection and use of personal information.

B. COPPA's "Actual Knowledge" Standard

SIIA supports the FTC's conclusion that Congress should not amend the COPPA statute's "actual knowledge" requirement. SIIA concurs that "actual knowledge" is more workable and provides greater certainty than applying a lesser "reasonable efforts" or "constructive knowledge" standard by which providers would be required to make an educated guess about which users may be children under the age of 13.

C. COPPA's Coverage of Evolving Technologies

SIIA agrees that the COPPA Statute and Rule are written broadly enough to encompass many new technologies without the need for new statutory language. Specifically, we agree that the terms "Internet," and "online service" broadly apply to mobile, or any service available over the Internet, or that connects to the Internet.

II. Expansion of the Rule's definition of "personal information"

With the proposed Rule change, the Commission proposes to use current authority in paragraph (F) to modify, and in certain cases, expand, upon the Rule's definition of personal information (PI) to "reflect technological changes."[2] SIIA strongly supports the objective of COPPA to protect the privacy and security of children under the age of 13, but in doing so, it is critical that the Commission not compromise the definition of what is, or is not, truly PI.

As a practical matter, the effort should be to balance the privacy and security objectives that the Commission seeks to uphold, without unnecessarily creating a regulatory

[2] 76 Fed. Reg. 59810 (Sept. 27, 2011)

framework that could inhibit the use of cutting-edge technologies to greatly enhance the customized, personalized user experience. SIIA believes the proposed modifications expand the definition beyond that which reasonably identifies an individual.

SIIA believes that the definition of PI should be limited to data that reasonably identifies an individual, such that it permits "the physical or online contacting of a specific individual"[3] per the text of the COPPA statute, and we therefore oppose the following proposed expansions of the definition of personal information.

A. Persistent Identifiers

SIIA is concerned with the proposed modification and expansion of the draft Rule's definition of PI to include "persistent identifiers" when these are not combined with personally identifiable information. Persistent identifiers in use today, such as IP addresses, a processor or device serial number, or a unique device ID do *not* constitute "personal information," unless a provider is actually combining the information with data that identifies a specific person. SIIA does not agree with the Commission's conclusion that persistent identifiers can inherently "permit the contracting of a specific individual." Without the collection and combination with personally identifiable information, as the rule currently applies, these persistent identifiers are not independently useful to identify a specific individual nor do they independently permit "the physical or online contacting of a specific individual," the established goal of COPPA. SIIA thinks that collection of one or more of these types of persistent identifiers does not compromise or degrade the privacy or security of an individual, and there is no reason to believe that it will in the future.

We are very supportive of the Commission's goals to ensure children's privacy and safety on the Internet, but expanding the definition of PI to include persistent identifiers poses significant challenges for companies to continue developing and providing innovative services. Indeed, we believe that this proposed definitional expansion provides more challenges and concerns to the existing privacy framework than it does solutions.

Specifically, this expansion would thwart the development of new, innovative technologies that customize the delivery of services and information. This approach would certainly cast the net too broad and force an unnecessarily wide range of providers to comply with COPPA's additional notice and consent requirements.

[3] 15 U.S.C. 312.2(c)

Devices will become *less* personal, not *more* personal

With this proposed rule change, the Commission clearly articulates its view that "increasingly, consumer access to computers is shifting from the model of a single, family-shared, personal computer to the widespread distribution of person-specific, Internet-enabled, handheld devices to each member within a household, including children." The Commission goes on to say that one or more unique identifiers associated with devices have created an environment where "operators now have a better ability to link a particular individual to a particular computing device."[4]

SIIA thinks that this vision inaccurately portrays the evolving nature of Internet-based technology, and it is an inappropriate basis on which to build a foundation of privacy regulations, either broadly or specifically just for children. On the contrary, we believe that the trend in the near future will shift further *away* from device linkage to specific individuals.

SIIA believes that the continued growth in cloud computing—which represents a shift to Internet-based content and that can be delivered seamlessly across a wide range of different devices—coupled with the increasing saturation and ubiquity of mobile computing devices that access the Internet, will rapidly lead to an environment where devices are *less* "personal" and *less* linked to a particular individual. Therefore, it is more accurate to suggest that we are shifting from a model of a single family-shared, personal computer to a model of internet-based device ubiquity, where individuals will have access to dozens of internet-based devices in a day, some that are personal, while most will likely be shared within a family or community of users.

For instance, we are already beginning to see households that have multiple computers, tablets, smart phones and televisions that all access the Internet. Family members migrate seamlessly between myriad devices to access music, video, applications and social networks. Expanded further outside of the home environment, it is also reasonable to expect that Internet-enabled devices, appliances and vehicles will proliferate, which likely will be used by a variety of individuals.

Persistent Identifiers Do Not Permit Contacting Specific Individuals

The Commission wants to include persistent identifiers as personal information because it thinks that these identifiers are like a home address or a telephone number in that "an operator who collects this information is reasonably likely to be able to contact a specific

[4] 76 Fed. Reg. 59811-59812 (Sept. 27, 2011)

individual, even without having collected other identifying information."[5] But this is incorrect.

The reality is that persistent identifiers are not contact information and would never be treated that way by people or institutions whose aim is to send a message to a specific individual. For example, if teachers in a school wanted to contact the pupils in their seventh grade classes to remind them of the due date for an important assignment, they would not choose to use persistent identifiers to convey that message. They would use one or more of the traditional elements of PI to convey that message. Home address, telephone number, or email address are traditional ways to contact individuals.

Another example illustrates the point that IP addresses and other persistent identifiers do not permit contacting specific individuals. When security firms and researchers detect a pattern of traffic from a particular IP address, they are not able to use this information to inform someone that his computer is infected. They can pass this information to internet service providers who can determine the subscriber to whom an IP address is assigned and can use the contact information in the form of an email address, home address or telephone to contact the subscriber to inform him that his computer is likely infected.

Simply put, persistent identifiers are not new technologically-advanced ways to accomplish the purpose of contacting children or any other specific individual. They should not be treated that way by COPPA or any other regulatory framework.

The Commission's only statutory basis for including persistent identifiers as personal information stems from the statutory definition of personal information as "individually identifiable information about an individual collected online including…any other identifier that the Commission determines permits the physical or online contacting of a specific individual."[6] But, as argued above, persistent identifiers, such as IP addresses, device IDs, and cookies that are not linked to PI, do not permit the physical or online contacting of specific individuals. For that reason, the Commission would be exceeding its authority if it were to conclude that persistent identifiers qualify as PI under COPPA.

Detecting Fraud and Preventing Cyber Attacks

With the proposed amendments to the Rule, the Commission itself notes the practical difficulties that might arise if persistent identifiers were treated as personal information, and tries to take steps to resolve them. It allows—without parental consent—the collection of persistent identifiers where they are used for "support for the internal operations of, or

[5] Id. at 59811
[6] Ibid.

protection of the security or integrity of, the Web site or online service." Examples of such internal operations cited by the Commission include "user authentication, improving site navigation, maintaining user preferences, serving contextual advertisements, and protecting against fraud or theft."[7]

While this is a positive step that recognizes the realities of how persistent identifiers are used by web sites, it may not go far enough. In particular, despite apparently allowing the use of persistent identifiers for protecting against fraud or theft, it in fact imposes significant barriers to the effective use of persistent identifiers for these purposes. It does this by requiring parental consent if persistent identifiers track individuals across websites.

This overly-broad requirement for parental consent for the collection of persistent identifiers that track users across web sites could diminish the effectiveness of services that detect and prevent fraud and security attacks. . Many Internet security service providers gather and analyze persistent identifier information across websites to detect and prevent fraud and security attacks. The collection and analysis of this cross-website information is essential in detecting and preventing these problems.

The proposed approach would mean providers of security services would not be allowed to track any user who visited a child-directed website unless they had first obtained verifiable parental consent. This proposal would greatly interfere with the efforts of providers of security services to protect child-directed and other websites.

The issue raised by this proposal is broader than its effect on child-directed websites and parental consent. It is whether consent should be required at all for collecting persistent identifier information that tracks users across web sites for the purposes of detecting and preventing fraud and security attacks.. It would be a step backward for the FTC to conclude in this proceeding that consent is required for persistent identifier information to be used to detect and prevent fraud and security attacks on any website or online service. In its draft privacy report, the FTC said that there are certain commonly accepted business practices "for which companies should not be required to seek consent once the consumer elects to use the product or service in question."[8]

One example was internal operations, which seems to be the same as the notion of internal operations outlined in the FTC's draft COPPA rule. Fraud prevention was another example cited by the FTC of a commonly accepted business practices where consent is not required. In that regard, the FTC noted that "online businesses also employ fraud detection services

[7] 76 Fed. Reg. 59812 (Sept. 27, 2011)
[8] *Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report (December 2010).

to prevent fraudulent transactions."[9] It seems as if the FTC was prepared in its draft privacy report to allow these fraud detection services to operate even across websites without the service operator or website needing to obtain consent. Indeed the services would not work very well if users could opt out of them.

In its comments on the draft FTC Privacy Report in February 2011, SIIA supported the principle endorsed in the Report that certain "commonly accepted business practices" involving the collection and use of information do not require consent.[10] As did Intel, Intuit and IBM. The idea that "fraud prevention" could be a legitimate use of information that would not require individual consent was also contained in the Use and Obligations Paper endorsed by the Center for Information Policy Leadership.[11]

SIIA urges the FTC to align the ideas of commonly accepted business practices in its privacy report and the notion of uses of persistent identifiers that do not require parental consent in the COPPA proposal. Operators of child-directed websites should not have to obtain parental consent in order to protect themselves and others from fraud and security attacks. SIIA urges the FTC to ensure that proposed changes to the COPPA Rule do not require parental consent for these uses of persistent identifiers.

B. Geolocation Information

Consistent with the reasoning above regarding persistent identifiers, SIIA does not believe that geolocation information is inherently PI and it therefore should not be a stand-alone element of the definition of PI. While the Commission argues that this information is personal because it is more precise than a home address, without the collection and combination with another type of PI that is truly personally identifiable, geolocation information does not lead to the ability to contact of a specific individual. In contrast, a home address does provide for the sending of mail or planned outreach because it is static.

SIIA urges the commission to recognize the value of integrating geolocation information for the provision of mobile services, but doing so in a way that is not combined with any form of personally identifiable information. We believe that it will continue to become more common for mobile apps to integrate *only* geolocation information for purposes of the internal functioning of a customized location-based learning or informational experience,

---

[9] Ibid.
[10] Comments of the Software & Information Industry Association on the Preliminary FTC Staff Report: *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers* (February 18, 2011).
[11] *A Use and Obligations Approach to Protecting Privacy: A Discussion Document*, The Business Forum for Consumer Privacy (December 7, 2009).

without the collection of other PI. If the information is not combined with any other PI, it is not useful for contacting of the user—either in person, via email or text, or any other practical type of contact—and therefore should not be considered an independent element of PI.

For example, a mobile app may collect *only* geolocation information to provide a visual glossary to help children identify the types of plants, insects and other elements that are indigenous to a particular ecosystem. It is hard to envision the privacy invasion that occurs in this circumstance where *only* location geolocation information is collected. It would be imprudent to create a regulatory barrier that prevents the development and use of these types of application over the next decade because of an inaccurate definition of PI that independently includes geolocation information under COPPA.

Again, while SIIA fully supports the goals of the Commission and COPPA to protect the privacy and security of children, expanding the definition of PI to include stand-alone geolocation information is casting the net too broadly. Rather, we recommend that geolocation information be considered an identifier that, when collected with another identifier that provides for contact, such as a an email address, would constitute PI under COPPA.

If the Commission moves forward with the proposed expansion of the definition, the new hurdle will unnecessarily stifle the use of customized, but anonymous, location-based services that are at the heart of mobile computing innovation.

C. Screen or User Names

SIIA does not agree with the Commission's recommendation to expand the definition of PI to include screen names and user names when they do not reveal an individual's email address. Specifically, the revised language categorizes screen and usernames as PI when used "for functions other than, or in addition to, support for the internal operations of the website or online service."[12] While the FTC advises that this is intended to exempt usernames that are "used solely to maintain the technical functioning of the website or online service," it also states that "an operator may allow children to establish screen names for use within a site or service," and that "screen names may be used . . . to identify users to each other . . ." without obtaining parental consent.[13]

Further clarification is required to confirm that interactive community based features on web sites and online services—for example playing games, and leaving comments on

[12] 76 Fed. Reg. 59810 (Sept. 27, 2011)
[13] Ibid.

games, videos, message boards and other site content—are included in the "internal operations" exemption. Indeed, expanding the definition of "personal information" to include screen name alone will create impractical, unnecessary barriers for the development of interactive, entertaining and educational web sites and Internet services for children. SIIA recommends that "screen name" be removed from the items of PI which, if combined with a persistent identifier, would render the identifier "personal information."

III. Expansion of the Rule's definition of "website or online service directed to children"

SIIA believes that the proposed revised definition of "website or online service directed to children" is overly broad. As defined by the Commission in the draft COPPA Rule, this would include "musical content" and "celebrities who appeal to children" among the indicia the FTC uses to determine whether a website or online service is "directed to children."[14] However, the Commission does not provide a sound explanation of how it would define which music and celebrities "appeal to children." This is overly broad because in many instances, music and celebrity talent appeal to both adults and children, often without distinction. The most likely result of this expanded definition will be the overly expanded scope of websites and online service to which COPPA would apply.

IV. Parental Notice and Consent

The COPPA Rule, as adopted and currently applied, has been effective in striking a balance between the obvious need to protect children online and the need to maintain the interactivity that benefits children's Internet experience. Interactivity and consumer end-use acceptability is the hallmark of the Internet, and the Rule recognizes this with its current notice and consent framework. Regardless of technological advancements since the enactment of COPPA, maintaining this balance is still just as critical today. SIIA supports the Commission's goal to expand the list of acceptable mechanisms to incorporate newer technologies and practices for obtaining consent, but we also support retention of the Rule's currently accepted methods, such as e-mail plus, as we believe this continues to be effective and efficient for both operators and parents alike.

A. Single Point of Contact for Notice

With this proposed Rule change, the Commission proposes that notice to parents should include contact information for *all* operators of a website or online service, rather than the current rule which permits designating a single operator as the contact point. SIIA strongly

[14] 76 Fed. Reg. 59814 (Sept. 27, 2011)

supports preservation of the current Rule allowing designation of a single point of contact for all operators of a Web site or online service.

While the goal of the Commission is to "aid parents in finding the appropriate party to whom to direct any inquiry," SIIA believes this modification will have the opposite effect. That is, this proposed changes is likely to *increase* confusion for parents as compared to allowing for a streamlined process where a single operator is designated as the contact point.

In explaining the impetus behind this proposed change, the Commission sites the mobile environment, specifically a "mobile application that may grant permission to an advertising network to collect user information from within the application." Regardless of the exact scenario, it is difficult to understand how a single point of contact would be less efficient or effective than multiple points of contact. Given how Internet-based services are evolving to become more commonly offered within broader services or platforms, it seems clear the proposed change would create *more, not less,* confusion for parents in cases where there are multiple operators on a single site or platform.

In addition to the obvious confusion, this new requirement would present operational challenges as well. The process of coordinating among multiple contacts and ensuring that multiple names and contact information remain current will become significantly more challenging. Given that the Commission has not effectively identified any issues parents have had with the single contact approach, we propose that the Commission retain the current single point of contact approach.

B. Recognition of a Streamlined, Centralized Parental Consent Service Provider

Consistent with the objective stated above to facilitate more efficient notice to parents through a single point of contact, and the objective of facilitating new efficient and reliable methods of consent, SIIA recommends that the Commission provide for the option of a streamlined, parental notice and consent mechanism.

That is, SIIA urges the Commission to enable the approach where multiple third-party operators provide notice and gain consent for collection and use of children's personal information through a single platform (including but not limited to a social network provider or an operating system platform), website or online service, which we will refer to as a "parental consent service provider." This provider, would provide notice and be able to obtain parental consent on behalf of multiple third-party operators, such as third-party sites, apps or services when certain conditions were met. Such conditions might include

requirements for notice, generic consent, further notice upon use of specific apps, and use restrictions on the information shared with apps under this approach, such as:

Notice: A single, designated "parental consent service provider" would provide notice to the child's parent that: (1) describes the designated operator's own information practices (if any); (2) states that third-party entities might collect, use, or disclose the child's personal information through the website or platform, and (3) generically describes the types of services that these third-party operators might provide.

Parental Consent: The "parental consent service provider" would be required to obtain verifiable parental consent for itself and third-party operators to collect, use, and disclose the child's personal information for the purposes described in the notice.

Additional Notice: The platform operator or the third-party operator would also provide the parent with additional notice the first time that the parent's child uses or installs the third-party operator's online service. This notice would include a brief description of the third-party operator's online service and a link to or an explanation of the third-party operator's online privacy policy for children's information (so that the parent could determine, for example, how to request that the third-party operator delete the child's personal information).

Use Restrictions: To the extent the third-party operator collects, uses, or discloses the child's personal information for purposes beyond support for the internal operations of the online service, the third-party operator would be responsible for separately providing notice and obtaining parental consent from the child's parent.

Such mechanisms would enable a single, designated operator (either a platform provider, or an independent party) to provide notice directly to parents either directly or through an interface, for a range of COPPA-covered web sites, applications or online services . This designated operator would be able to provide verifiable parental consent for third-party operators to collect, use, and disclose the child's personal information for the purposes described in the notice, and any of its own practices if it also engages in collection of children's information.

We believe this approach could be effective not only for independent third-party web sites, but also platforms such as operating systems of mobile devices or social networking sites that run various applications and services within an Internet-based platform. Of course, a critical element of this approach would be to ensure that the platform, or independent parental consent service provider, is not liable for the individual covered operators, but rather the operators would be responsible for abiding by the parental consent service

provider's notice and use policies. To the extent the third-party operator collects, uses, or discloses the child's personal information for purposes beyond support for the internal operations of the online service, the third-party operator would be responsible for separately providing notice and obtaining parental consent from the child's parent.

C. Proposed Elimination of the Sliding Scale Approach ("e-mail plus")

SIIA does not fully understand or agree with the Commissions concerns about the lack of reliability of "e-mail plus." We believe that elimination of the sliding scale approach would be impractical and counterproductive for the following three reasons.

First, in establishing the sliding scale approach as temporary when the initial COPPA Rule was written, the Commission explained that this approach would be replaced as "the Commission determined that more reliable (and affordable) consent methods had adequately developed."[15] However, in proposing to eliminate the sliding scale approach at this time, the Commission has essentially pointed out that a range of such reliable and affordable methods are still *not* available. In the Proposed Rule the Commission has now placed the blame on e-mail plus for stifling technological development, by asserting that "the continued reliance on e-mail plus has inhibited the development of more reliable methods of obtaining verifiable parental consent."[16]

We strongly disagree with this conclusion. Rather, we believe that reliance on e-mail plus has continued because of its effectiveness as applied around the world, and the lack of other technologies that are any more effective or nearly as efficient. As stated above, we are confident that innovative applications of technology will enable new methods of consent, but we do not believe e-mail plus should be eliminated until such time as these alternative mechanisms are truly widely available.

Second, the proposed elimination is short-sighted in failing to account for how new technologies can be combined with e-mail notification to provide for more reliable notice and consent that is e-mail-based. For example, the aforementioned Parental Consent Service Provider proposal—for an intermediary parental notice and consent mechanism—would be best served by integrating an e-mail plus like process. This would include the delivery of notice via email and requirement of parental consent through an already established third-party account that is maintained by the parent, in the parent's name.

Finally, the notion of easy circumvention of e-mail consent should not be so broadly assumed. Most children under the age of 13 are not sufficiently technologically

[15] 76 Fed. Reg. 59819 (Sept. 27, 2011)
[16] Ibid.

sophisticated to setup an email account, let alone do so with the intent to falsify parental consent. Indeed, only the most sophisticated users under the age of 13, and those intent on disobedience, would fit into this category—a very small category. Therefore, as a method that balances the need to protect children online with the need to efficiently enable parental notice and consent, e-mail plus has significant usefulness and reliability in many instances around the world, both today and into the foreseeable future.

Again, SIIA recognizes and agrees with the FTC's desire to see new and more sophisticated methods developed over time, but we believe it would be very harmful to eliminate e-mail plus until such time as these methods develop and parents become more comfortable with them. Instead, we urge the Commission to allow e-mail plus to be preserved for the vast majority of applications where it is highly efficient and reliable.

D. Commission and Safe Harbor Approval of Parental Consent Mechanisms

Companies need flexibility to identify additional reasonable means of obtaining consent over time, but the proposed new notice and comment process may not be the best means of supporting rapid innovation needed in this space. That is, the proposed process by which an application is submitted and a comment and approval process ensues seems overly rigid and not keeping with the pace of advancing technology. Nor does this approach seem to be considerate of market competition. Therefore, we would encourage the Commission to consider innovative mechanisms for obtaining verifiable parental consent to be used in the market pending Commission review, or at the least to allow these mechanisms to receive expedited review. It might be possible to develop principles that could govern when such pre-review market use or expedited proceedings would be appropriate.

SIIA encourages the FTC to explore how to engage parents and facilitate the provision of consent as technology evolves, so as to provide wider options for children to benefit from the Internet in a safe way. For example, the Commission could explore how parental controls might be used to provide verifiable parental consent, especially in the mobile space where parents are purchasing the connectivity service and the device.

E. Password Reminder (or Reset) Exception

As explained in the FTC's COPPA Frequently Asked Questions (FAQ, #30) guidance, the Commission currently allows an exception for "collecting a child's and a parent's online contact information in order to send the child periodic communications, such as online newsletters, site updates, or password reminders." The Commission explains that multiple contacts with a child are acceptable provided that the operator "make reasonable efforts to

ensure that the parent receives notice and is informed of the opportunity to opt-out of further use of the information collected."

However, requiring parental notification and opt-out consent for password reminders or resets seems to be an unreasonable burden on operators, including providers of educational services. In some cases, these operators want to collect a child's email address for the sole purpose of continuing to make service available to a child who may have forgotten his password. The use of the email address is intended purely to allow the site to manage its internal operations and to continue to provide services to its users. In these cases, the need to obtain parental email in order to satisfy the parental notice and opt-out requirement can be an unnecessary barrier that could result in the loss of service to the child. The Commission has also recognized this and provides for conditions under which collecting a child's email purely for the purpose of password reminders or resets would not require the operator to notify the parent and provide them with an opt-out opportunity (#45).

SIIA urges the Commission to build on and codify the principles established in FAQ's 30 and 45 to make clear that collecting a child's email purely for the purpose of multiple password reminders and resets would not require the operator to notify the parent and provide them with an opt-out opportunity.

V. School-based educational partners and providers of educational materials and services

In supporting the goals of COPPA, SIIA encourages the Commission to take steps to ensure that it is applied as efficiently as possible with respect to school-based educational partners and other providers of educational materials and services. COPPA should not become an unnecessary barrier to students under age 13 who are seeking access to teaching and learning opportunities important to their formal, academic education, whether accessed within the school or outside of it. To this end, we make the following two recommendations:

A. Clarification of distinction for educational partners with schools

COPPA guidance currently allows schools to act as agents for parents in providing consent for the online collection of students' personal information within the school context, whether that educational experience is accessed at school or outside of school, from a school device or from a personal device. SIIA urges the Commission to codify this allowance.

Many school districts contract with third-party providers to offer online programs solely for the benefit of their students and for the school system, e.g., homework help lines, online adaptive courseware, or web-based testing services. COPPA does not currently apply to the website operator's collection of personal information from participating children where a school has contracted with an operator to collect personal information from students for the use and benefit of the school, and for no other commercial purpose. Thus, the operator is not required to obtain consent directly from parents, and can presume that the school's authorization for the collection of students' personal information is based upon the school having obtained the parents' consent. (Note: Under the current guidance, the operator should provide the school with full notice of its collection, use, and disclosure practices, so that the school may inform parents of these practices in its Acceptable Use Policy).

SIIA strongly supports this current distinction, outlined in FTC guidance (FAQ #54 and #55) regarding the special status of schools and website operators that provide online services to them. The institutional structures in place – with instruction via the school as an intermediary – provide ample oversight and review without an additional layer of parental consent. Those institutional structures include teachers and other school administrations, the classroom setting, the adoption and review process of instructional materials, the review of third-party information practices, etc.

Therefore, SIIA urges the commission to codify this distinction in the regulation to ensure all stakeholders have certainty about these regulations, rather than relying on less formal and less dependable FAQ guidance.

B. Creation of an Educational Exception

SIIA encourages the Commission to consider ways to create an exception for educational providers to prevent students from facing an unnecessary hurdle of notice and consent in cases where the website or online service is academic in nature. Such an exception could fall under Section 1303(b)(2)(c)(ii) of the statute that provides the Commission with authority to craft exceptions "taking into consideration the benefits to the child of access to information and services." This exception is critical to minimize the barriers to dynamic educational opportunities that may prevent students from accessing just-in-time opportunities as academic educational opportunities extend beyond the school through anytime, anywhere virtual learning.

While it is critical to codify FAQs #54 and #55 regarding the allowance of schools to act as agents for parents in providing consent for collection of students' personal information within the school context, this additional exception would address the alternative scenario that academic experiences will be increasingly occurring independent of the school,

anytime and everywhere through the use of mobile technologies and virtual learning. In addition, academic learning will be increasingly decentralized and disaggregated as students leverage just-in-time content and instruction, often at a granular level to meet a specific need.

For example, a rural student may have an hour-long bus ride home from school, be studying on their mobile device, and have occasion to contact an online tutor or connect to online, interactive educational resources at that moment to help with a specific problem. Multiple related situations could occur during that time, each requiring their timely access to an online learning opportunity requiring personal information. Lack of an exception as suggested here will present an increasingly significant barrier to important academic opportunities for students under age 13.

Such an exception would recognize the unique nature of education. Public policies must encourage education, not create barriers. The public and individual good is best served by enabling the education of all citizens and children. Our regulatory policies should not be neutral between online entertainment and online learning. They should enable students to learn, and encourage providers to deliver educational content and instructional services. However, placing the full set of COPPA requirements on education providers has a chilling effect on what is, and should be recognized as, a public good.

VI. Conclusion

Again, thank you for the opportunity to provide comment on this important issue. SIIA shares the Commission's commitment to helping maintain a safe, secure online experience for children and to ensure that COPPA continues to meet its originally stated goals, even as technologies change. If you have questions about these comments or would like to discuss further, please contact David LeDuc, Senior Director, Public Policy, at dleduc@siia.net or 202-789-4443

Sincerely yours,

Ken Wasch
President