Software & Informa
Industry Associa

September 24, 2012

Federal Trade Commission
Office of the Secretary
Room H-113 (Annex E)
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

RE: COPPA Rule Review, 16 CFR Part 312, Project No. P104503

Thank you for the opportunity to comment on the Supplemental notice of proposed rulemaking ("Supplemental NPRM") issued on August 6, 2012. The Software & Information Industry Association (SIIA) continues to share the Commission's commitment to maintain a safe, secure online experience for children, and to ensure that the Children's Online Privacy Protection Act (COPPA) continues to meet its goal 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.

I. Introduction

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.

SIIA understands and appreciates the Commission's observations regarding changes in technology that make it more commonplace for child-directed sites and services to integrate social networking and other plug-in features into their websites in order to provide the website with content and functionality. Further, we are supportive of the goals of the Commissions goal to protect children from third-party plug-ins, social networks and any other third party service that collects personal information.

However, the inappropriately broad expansion of the statute's definition of personal information, combined with the increasingly broad definitions of "operator" and "web site or online service directed to children," along with the new "reason to know standard" and requirement for "child-friendly mixed audience" sites and services to age screen, create a broad regulatory framework that dramatically exceeds the scope of COPPA and will most certainly stifle innovative Internet-based offerings—not just for sites and services directed at children under 13, but much more broadly.

In SIIA's view, a third party plug-in or a first-party operator of a web site should be responsible under COPPA only to the extent that it is otherwise subject to COPPA because either it has actual knowledge that it collected traditional personally identifiable information from a child or it offers a kid-directed service. The Commission also should clarify that any operator, including operators of third-party plug-ins, can take advantage of exceptions set forth in the Commission's rules, including exceptions

around the definition of personal information. With respect to that definition, we urge the Commission to reconsider its treatment of persistent identifiers as personally identifiable information triggering COPPA requirements.

Please find below detailed comments and recommendations in response to the Supplemental NPRM. While the comments address the recently proposed changes together due to their interdependence in practical application, we have attempted to provide recommendations corresponding with specific proposed modifications outlined in the Supplemental NPRM to help the Commission address its goals without breaking-down the current and burgeoning Internet business models.

II. Proposed expansion of "personal information" to Include persistent identifiers creates an unworkable regulatory construct for COPPA.

As we stated in our last comments in December 2011, we continue to strongly disagree with the Commission's proposal to include persistent identifiers within the definition of personal information.[1] As we stated at that time, persistent identifiers do not meet the definition established by Congress when it enacted COPPA because persistent identifiers do not independently by themselves allow for the identification or contacting of a specific individual.

Contrary to the stated conclusions of the Commission, by themselves, most persistent identifiers are passive and anonymous and should not alone be treated as "personal 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,"

[1] SIIA comments, Dec. 2011

unless a provider is actually combining the information with data that identifies a specific person, as the current COPPA rule recognizes. Indeed, while it is true that persistent identifiers, such as a cookie that also contains a customer number, when stored with other personal information such as first or last name, could make it possible to identify and contact a particular individual, the characterization of persistent identifiers independently as personal information remains far off course.

As has been pointed out by a number of commenters in response to the initial proposed rule change in 2011, many sites and services collect *only* anonymous persistent identifiers and would therefore effectively meet the threshold of being an "operator" without actually collecting any personal information necessary—e.g. name and email address—to provide notice and obtain consent. It is without question that this construct leads to collection of *more* personal information from children, not less.

More broadly, SIIA continues to strongly disagree with one of the fundamental conclusions of the Commission that appears to be at the heart of this proposed definitional expansion. That is, the Commission's conclusion that particular devices are associated with particular individuals, and the collection of persistent identifiers, such as IP addresses, therefore permits identification and direct contact with specific individuals online. The Commission clearly articulated this perspective in the 2011 proposed rule change, stating 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 also went 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."[2]

On the contrary, as we articulated in our 2011 comments, SIIA's work with our member companies—a wide range of companies that are market leaders in delivering software, apps and digital content products and services—has led us to confidently conclude the opposite. That is, it is clear to us that the proliferation of Internet-connected devices is quickly leading to the *depersonalization* of devices.

Further, while the proposal to include persistent identifiers caused SIIA and the technology industry significant concerns when initially proposed in 2011, the level of potential harm to innovative offerings has increased this concern exponentially, as the Commission is now casting it much more broadly by expanding the definition of an "operator" as well as a site or service "directed to children," and proposing that mixed audience sites be required to begin age screening for children under 13.

As flawed as it was to apply an expanded personal information definition in the currently narrow context of COPPA covered entities, the other expansions contained in the Revised NPRM would make it virtually impossible for companies of all types to function as they do today without having to follow COPPA's requirements unnecessarily or dramatically scale-back offerings. For example, a site or service (or mobile application) that does not in any way target children under 13, and does not by any practical and legitimate assessment collect "personal information," but that does use persistent identifiers for behavioral advertising other business purposes, would quite

[2] Notice of Proposed Rulemaking and Request for Comment, Children's Online Privacy Protection Rule, 76 Fed. Reg. 59811-59812 (Sept. 27, 2011)

likely be swept into the scope of COPPA's verifiable parental notice and consent requirements.

Clearly, the proposed regulatory construct, if implemented, will extend far beyond the statutory intention of COPPA.

III. The proposed modification to the Rule's definition of "operator" is overly-broad, and it places an unworkable responsibility on operators of sites and services well beyond the scope of COPPA.

While we understand the Commission's goal in exploring the partnerships between operators and embedded services, and the objective to ensure that COPPA notice and consent requirements are not overlooked as a result of innovative Internet-based offerings, we are very concerned that the proposed modifications to the Rule's definitions of an "operator of a child-directed site or service" and definition of "web site or online service directed to children" are unworkable on many levels.

As a general matter of interpreting COPPA, SIIA strongly believes that web sites and services that are *not* targeted to children under 13, and do not receive data collected by third party services from children, are clearly outside the scope of COPPA. Therefore, these sites or services should not have to provide notice and consent for ad-networks or plug-ins offered as part of that site or service that may collect information from users. Additionally, services such as social networks that "age gate" access to their platforms should not be subject to COPPA requirements.

SIIA disagrees strongly with the Commission's proposed definition of "operator," which would make a first-party site or service responsible for the COPPA compliance of integrated third-party services that gather personal information (such as plug-ins, software downloads, or advertising networks) over which the first-party retains no control. In support of its position, the Commission states that the site operator "is in an appropriate position to give notice and obtain consent from parents where any personal information is being collected from its visitors on or through its site or service," and that the site operator "is in the best position to know that its site or service is directed to children and can control which plug-ins, software downloads, or advertising networks it integrates into its site."[3]

SIIA disagrees with these assumptions to the extent the Commission expects that a first-party site or service is in the best position to know whether and how a third-party service integrated into its site or service is collecting and handling personal information gathered via the plug-in, and whether the third-party service's practices are COPPA compliant. A first-party should not be required to constantly monitor these third-party services – a task which would prove unduly burdensome (both time consuming and expensive) – in order to keep abreast of these often changing practices, and so should not have to provide notice and obtain verifiable parental consent for ad-networks or plugins offered as part of that site or service that may collect information from users.

IV. The Commission's proposal to make third parties qualify as "operators" under COPPA by creating a "reason to know" standards is both an inappropriately broad expansion of the statute and technically impractical.

[3] Federal Trade Commission, Supplemental Notice of Proposed Rulemaking and Request for Comment, Children's Online Privacy Protection Rule, 77 Fed. Reg., 46644 (August 6, 2012)

The incorporation of the proposed "reason to know" standard within the definition of a "web site or online service directed to children" presents significant new responsibility for third-party ad-networks or plug-ins to also provide notice in the cases where they become aware, or merely have reason to be aware, that their offerings are incorporated into child-directed sites or services.

As the Commission has recognized, "the strict liability standard applicable to conventional child-directed sites and services is unworkable for advertising networks or plug-ins because of the logistical difficulties such services face in controlling or monitoring which sites incorporate their online services."[4] SIIA agrees with this obvious conclusion, and that it equally would apply to social networks and platform providers. But the expansive approach proposed in the Revised NPRM to hold third-parties accountable when they have a "reason to know" is still very flawed because this approach would impose liability where there is neither intent to collect information from children, nor actual knowledge that any particular user is a child. So the construct is counter to the Commission's objective of preventing information collection from children, and it would lead to information being collected, such as name and email address in order to provide notice and seek consent.

As articulated by the Commission, the combination of these proposed definition modifications will "hold the child-directed property to be a co-operator equally responsible under the Rule for the personal information collected by the plug-in or advertising network will help ensure that operators in each position cooperate to meet their statutory duty to notify parents and obtain parental consent."[5]

[4]Ibid., 46645
[5] Ibid

In exploring the relationship between "operators" and third-party plug-ins, it appears that the Commission has overlooked some critical technical elements of these relationships. That is, providers of web-based—or app-based—plug-ins usually design offerings so that sites and services wishing to incorporate them do not need to establish a business relationship. For instance, video streaming plug-ins could practically be expected to be offered in a way where they can be embedded quickly and easily by any web site operator. And in the case of a social network, including plug-ins that link back to the network are also implemented in a way where the entities operate very separately, and without a formal relationship, let alone a contract. So in many of these cases, the plug-in, social network or other platform operator could neither have any relationship with the site or service, nor would it have access to that user to provide notice and seek parental consent. Further, as discussed above, the greatest difficulties created by the Revised NPRM's notice and consent construct hang on the inappropriately broad definition of "personal information," which includes persistent identifiers independently, when they are clearly *not* personally identifiable.

Therefore, SIIA strongly objects to the two proposed constructs established in the Revised NPRM: (1) the "co-operator" construct which assumes a relationship between parties that most likely does not exist, and (2) the proposal for operators of third-party analytics services, advertising networks, plug-ins, platform providers and social networks that do not intentionally target their services to children, to have independent COPPA notice and consent obligations under any circumstances.

V. The proposed requirement for operators of "child-friendly mixed audience sites" to take an affirmative step to attain actual knowledge of child users would inappropriately expand the scope of COPPA and place an undue burden on a wide range of sites and services not directed to children.

As clearly articulated by the Commission, this proposed modification of the definition of "website or service directed to children" is intended to effectively "require operators of these child-friendly mixed audience sites and services to take an affirmative step to attain actual knowledge if they do not wish to treat all visitors as being under 13."[6] This proposed change will expand the application of COPPA very broadly, based on an ambiguous definition of mixed audience sites.

SIIA understands and agrees with the request, as explained by the Commission was submitted by Disney to voluntarily utilize age-screening on mixed audience sites to avoid those sites from possibly being treated as COPPA covered and therefore alienating older users. However, the mandatory extension of this approach established by an impractically ambiguous definition of what might constitute an operator of a site "with child-oriented content appealing to a mixed audience, where children under 13 are likely to be an over-represented group" inappropriately expands the coverage of COPPA and the practical definition of what a COPPA-covered operator is.

As a practical matter, the number of sites and services that would be required to age screen and adopt notice and consent mechanisms would be very high. Further, particularly when combined with the extraordinarily broad definition of personal information being proposed by the Commission, the result would be a dramatic increase in the number of sites that need to age screen and implement COPPA compliant notice

[6] Ibid., 46646

and consent for merely providing behavioral advertising, collecting persistent identifiers or even integrating plug-ins that do this. Despite the collective goals of industry, consumer advocates and the Commission to encourage less information collection, this proposed change would have the opposite effect.

VI. Application platforms, such as app stores or social networks serving as platforms on which applications may be obtained and/or used, should *not* be characterized as "operators" under COPPA, but the Revised NPRM leaves this unclear.

Yet another major concern created by the ambiguity of the proposed definitional changes in the Revised NPRM is the possibility that the definition of "operator" could be applied to cover entities such as app stores or social networks serving as platforms on which applications may be obtained and/or used. While we are hopeful that this is *not* the intent of the Commission, there is clearly sufficient ambiguity in the proposed definition that the Commission could seek to characterize a platform, such as an app store making an application available which subsequently collects "personal information," as an "operator" because it has somehow "benefited" from being able to offer the application.

SIIA strongly opposes this possible interpretation of an "operator," as it would represent a dramatic expansion of the COPPA statue and threaten a burgeoning model of platforms that is indeed beneficial to the delivery and use of applications by all consumers, including but not limited to children. We offer the following insights into why this interpretation would be impractical and counterproductive to the goals of COPPA and the Commission.

First, extension of COPPA operator responsibilities to an app platform is often not practical technically, as it would require platforms to undertake extensive additional steps to review applications that would not be possible for most companies to satisfy. Looking closely at mobile app stores as platforms provides a good example of this. While app developers are fully cognizant of the specific features of their apps and how they could apply to COPPA, the platforms on which these apps may be offered do not have access to such details. Further, with an increasingly ambiguous set of definitions regarding what constitutes "personal information" in the COPPA context, or whether an app is "directed to children," only the entity offering the application could reasonably be expected to know this.

Second, going beyond a platform's limited knowledge at the time the application is offered, apps are incredibly dynamic and becoming more so as this industry develops. That is, apps are frequently being changed and upgraded by developers to improve the functionality to adapt to users' needs—indeed, mobile apps today are much more frequently updated than traditional software applications running on desktop computers. Therefore, even if it were practical for a platform to effectively serve as a COPPA operator in offering a consumer initial access to an app, the ongoing ability for that platform to continually serve as an "operator" in perpetuity would be a completely inconceivable undertaking.

Third, and perhaps most importantly, it is imperative that the Commission avoid overregulation of platforms that could serve as a disincentive for them to allow apps that could be perceived as targeted to children. Today, we are experiencing an exploding market for apps that run on smartphones, tablets and social networks, and various other platforms. This is despite the fact that these are all very new

technologies—all being introduced within the last decade, and many just in the last few years.

At the same time, the Commission has encouraged platforms to play a greater role as a gatekeeper for users. Specifically, in the FTC Staff Report, Mobile Apps for Kids, the Commission explicitly identifies app platforms as "gatekeepers of the app marketplace," and urges that they "should do more."

SIIA urges the Commission to recognize that the construct of platforms is still very new, and quite likely to continue evolving. Today, apps that run on mobile devices are often made available in mass quantities from a single "store," offered by the provider of a mobile operating system. However, as devices, platforms and the app developer industry all continue to evolve; it is entirely possible, if not likely, that the platforms of tomorrow will look very different. For instance, it is entirely possible that operating system providers would no longer find it to be in their best interest, or in the best interest of their users, to offer apps through a "store." Indeed, software for desktop computers has been obtained by consumers on the Internet through a much more decentralized model for more than a decade, and overregulation of platform providers as an "operator" could very quickly begin to stifle innovation and most certainly drive consumers, app providers, and platform providers to shift away from this approach.

As we have urged on many occasions, regulatory constructs must not be developed today which are based on a snapshot of current technology in a dynamically evolving information and communications technology ecosystem that is likely to be very different tomorrow.

However, while we object to the possible interpretation of the Commission's revised proposal to require app stores and social networks to be characterized as "operators" and therefore possibly liable for the COPPA compliance of the apps offered on their platform, we do think it desirable for the Commission to provide the opportunity for apps to work with platform providers, in a voluntary manor, to satisfy their COPPA obligations. That is, where it is technically feasible, platforms might want and be able to simplify the process for parents to provide verifiable consent for the use of various child-directed apps made available on the platform, as described in SIIA's previous comments in 2011. In such a case, they should be able to do this without thereby becoming "operators" subject to COPPA requirements. SIIA strongly believes that in this scenario the COPPA obligations should continue to remain with the app provider, not with the platform, and liability for failure to live up to those obligations should remain with the app provider.

VII. The broad regulatory construct proposed in the Revised NPRM is likely to challenge application of COPPA to Internet-based educational materials and services.

In our comments regarding the proposed COPPA Rule chance in December 2011, SIIA encouraged 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 Internet-based educational materials and services. SIIA believes now, as we did then, that it is imperative that COPPA 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.

In light of the broad regulatory construct proposed in the Revised NPRM, we are further concerned that many providers of online learning opportunities will cease or curtail

their efforts, or at least limit dramatically the innovation and customization of learning in current and future offerings. Further, we are concerned that many online learning opportunities will be degraded by the limitations of the use of what might be interpreted (regardless of whether intended) as "personal information," even if not personally identifiable. Such examples could include a student's learning interests, performance, past experiences, etc. as determined through their online learning experience.

To help limit the negative impact on innovation in this area, and to help the Commission implement COPPA as efficiently as possible with respect to school-based educational partners and other providers of educational materials and services, SIIA again urges the Commission to: (1) codify the current guidance allowing schools to act as agents for parents in providing consent for students, and (2) 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.

VIII. Summary of Recommendations

1. Definition of personal information – The Commission should further reconsider its proposed expansion of "personal information" to include persistent identifiers. Since persistent identifiers do not inherently identify a specific individual, the Commission should continue to define personal information more narrowly to include persistent identifiers only where they are used in conjunction with another element of personal information and could therefore be reasonably associated with a specific individual, rather than including persistent identifiers as an element of personal information unless otherwise exempted for "internal operations."

2. First-party operators – Contrary to the Commissions belief, operators of sites and services are *not* "in an appropriate position to give notice and obtain consent from parents where any personal information is being collected from its visitors or through its site or service." Other than applied in a narrow, "child-directed" site or service, first-party sites, such as publishers, cannot reasonably be thrust into a position of being responsible to monitor and control third-party content, particularly when the "personal information" collected is merely the use persistent identifiers, or in a case where the third-party is the entity collecting any personal information. Therefore, the Commission should (1) make it clear that persistent identifiers do not constitute personal information in this context, and (2) clarify that a first-party site or service would certainly not be liable should a third-party service or plug-in make a representation of compliance that it does not uphold.

3. Third-parties – The construct proposed by the Commission in the revised NPRM would effectively make third-parties qualify as "operators" under COPPA, therefore making them independently responsible under COPPA if they "have reason to know," they are collecting "personal information" from a site or service that is "directed to children." This is a bridge too far. As discussed above, providers of web-based plug-ins intentionally design offerings so that they do not require a relationship with first party sites and services—and in most cases do not have a relationship with the users. Further, as discussed above, the difficulties created by the Revised NPRM hang on the inappropriately broad definition of "personal information" to include information that is not personally identifiable. Therefore, the commission should abandon the proposed application of a "reason to know," standard for third parties, particularly in cases where the information collected is only persistent identifiers.

4. Age screening – This proposed requirement for mixed-audience sites and services to "age-screen" is a sweeping expansion of COPPA beyond the statutory intent of the law. This proposal appears to establish a regulatory construct where a site that is not targeted to children and does not actually collect any identifiable information, would regardless be treated as a COPPA operator. In order to avoid inappropriately extending the scope of COPPA and forcing an extremely wide range of sites and services to comply with COPPA notice and consent regime—beyond those "directed to children" as intended by the statute—the Commission should withdraw the proposed requirement. At a minimum, this requirement should not be applied to sites where the collection of "personal information" is no more than utilization of persistent identifiers, either directly within the site or by a plug-in.

5. Platforms – The Commission should clarify that general audience platforms, e.g. app stores or social networks offered to a broad audience, are not swept into the definition of "operator" in a regulatory construct that would make them responsible for complying with COPPA notice and consent requirements. Requiring platforms to serve as "operators" in this context would inappropriately expand COPPA and provide an unworkable framework for platforms.

Separately, while platforms should not be characterized as "operators" under COPPA, the Commission should permit platforms, websites or third party services to provide the opportunity for apps to voluntarily work with platform providers to satisfy their COPPA obligations. The goal of this approach would be to streamline and centralize notice and consent, where practical, through a common platform that is able and willing to assume the role for the benefit of its customers. They should be able to do this without effectively becoming "operators." For this to be a workable framework, it is imperative that this be a voluntary construct for platforms and app providers that desire to work

together in helping meet COPPA obligations. Liability for compliance with these obligations would appropriately remain with the app provider, as the entity that is responsible for implementing the technology that collects any personal information.

6. Educational materials and services – With schools increasingly shifting to digital educational materials for the benefit of providing a superior, customized learning experience tailored to students, SIIA encourages the Commission to take steps to ensure that COPPA is applied as efficiently as possible with respect to school-based educational partners and other providers of educational materials and services. Specifically, SIIA recommends that the Commission:

> (1) Codify the current guidance allowing 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, and (2) 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.

Again, thank you for the opportunity to comment on this very important issue. If you have questions or would like to discuss, please contact David LeDuc, SIIA Senior Director for Public Policy, at dleduc@siia.net or (202) 789-4443.

Sincerely yours,

Ken Wasch
President