December 23, 2011

<u>BY ELECTRONIC FILING</u>

Mr. Donald S. Clark
Federal Trade Commission
Office of the Secretary, Room H-113 (Annex E)
600 Pennsylvania Avenue, NW
Washington, DC 20580

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

Dear Secretary Clark:

The Entertainment Software Association ("ESA")[1] has been an active participant throughout the Commission's proceeding assessing its rule implementing the Children's Online Privacy Protection Act ("COPPA Rule").[2] We thank the Commission for its careful consideration of our submissions in the Commission's COPPA roundtable and its 2010 request for comments,[3] and we appreciate the opportunity to expand upon our earlier participation and to respond to the Commission's proposed revisions to the COPPA Rule.

ESA and its members take our responsibility to protect children's privacy and safety online seriously, and we have a long history of developing innovative solutions to promote

[1] The ESA is the U.S. association exclusively dedicated to serving the business and public affairs needs of companies that publish computer and video games for video game consoles, personal computers, and the Internet.
[2] Children's Online Privacy Protection Rule, 76 Fed. Reg. 59804 (Sept. 27, 2011).
[3] *See* Transcript, *Protecting Kids' Privacy Online: Reviewing the COPPA Rule* (June 2, 2010), http://www.Commission.gov/bcp/workshops/coppa/COPPARuleReview_Transcript.pdf; Letter from Kenneth L. Doroshow, Senior Vice President & General Counsel, ESA, to Mr. Donald S. Clark, Secretary, Federal Trade Commission (June 30, 2010), http://www.Commission.gov/os/comments/copparulerev2010/547597-00048-54857.pdf (hereafter "June 2010 Comments").

Entertainment Software Association • 575 7TH Street, NW • Suite 300 • Washington, DC 20004 • 202.223.2400 • 202.223.2401 FAX

privacy, safety, and parental involvement in the online video game environment. We highlighted a number of these efforts in our June 2010 COPPA Comments. More recently, the Entertainment Software Rating Board ("ESRB"), which ESA founded in 1994, partnered with CTIA[4] to develop a new mobile application rating system that six mobile application storefronts will voluntarily support as part of their app submission process.[5] The system will utilize the comprehensive and parent-trusted age rating icons that ESRB assigns to computer and video games in order to provide parents and consumers reliable information about the age-appropriateness of applications.[6] Commissioner Mignon Clyburn of the Federal Communications Commission commended this effort as helping "parents and consumers make fully informed choices about mobile applications purchases."[7]

The video game industry values the trust that it has earned with parents and regulators over the past two decades and will continue to explore how best to provide children a wide variety of age-appropriate, interactive experiences online while also encouraging parental involvement. We believe that the COPPA Rule has effectively served the goal of ensuring that parents are well informed about their children's online activities while also affording operators

[4] CTIA — The Wireless Association is an international nonprofit membership organization that represents the wireless communications industry.
[5] Press Release, "CTIA — The Wireless Association® and ESRB Announce Mobile Application Rating System" (Nov. 29, 2011), http://www.esrb.org/about/news/downloads/CTIA_ESRB_Release_11.29.11.pdf.
[6] Fed. Trade Comm'n, *Marketing Violent Entertainment To Children: A Sixth Follow-up Review of Industry Practices in the Motion Picture, Music Recording & Electronic Game Industries*, at iii (Dec. 2009), http://Commission.gov/os/2009/12/P994511violententertainment.pdf (stating that "[o]f the three entertainment sectors, the electronic game industry continues to have the strongest self-regulatory code").
[7] Statement of Commissioner Mignon L. Clyburn on CTIA's Mobile Application Content Rating System (Nov. 29, 2011), http://www.thedcoffice.com/late_releases_files/11-29-2011/News.pdf.

sufficient flexibility to offer innovative and engaging websites and online services that children can enjoy and that parents feel confident allowing their child to experience.[8]

To this end, we believe the Commission has achieved a proper balance in at least four important respects:

- *First*, ESA supports the Commission's decision to not seek a statutory amendment that would raise the COPPA age threshold to cover teens. ESA agrees with the Commission that, although "COPPA's parental notice and consent model works fairly well for young children . . . it would be less effective or appropriate for adolescents."[9]

- *Second*, ESA believes the Commission appropriately retains the "actual knowledge" standard for operators of general audience websites that collect personal information from children under the age of 13. This approach is not only consistent with the congressionally mandated standard, but will also continue to protect children's privacy online, while also providing clear, practical guidance to industry. A lesser "reasonable efforts" or "constructive knowledge" standard would create significant regulatory uncertainty with minimal countervailing benefit, particularly in light of the proposed expansion of the definition of "personal information."

- *Third*, ESA enthusiastically supports the Commission's proposal to clarify that operators do not "collect" personal information from children where they employ technologies that are "reasonably designed" to filter all or virtually all personal information from children's online posts. As ESA explained in its June 2010 Comments, this standard will facilitate innovation in filtering technology and help ensure the continued availability and viability of chat and other communication tools that are appropriate for young audiences.

---

[8] A recent study found that parents want their children to be able to connect with peers, classmates, and family members through popular communications and social networking websites. *See* Danah Boyd, et al., "Why Parents Help Their Children Lie To Facebook about Age: Unintended Consequences of the 'Children's Online Privacy Protection Act,'" FIRST MONDAY (Nov. 2011), http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075. Among those parents surveyed who knew their child joined Facebook when they were under the age of 13, 68 percent reported that they helped their children to create the account, which involved lying about the child's age so that the child could gain access to Facebook in violation of the site's terms of service. *Id.* The study also found that the majority of parents (59%) believe getting parents involved in children's online activities should be the primary focus of efforts to keep children safe online, compared to only 12 percent who believe this focus should be on restricting children's access to online services. *Id.*

[9] Children's Online Privacy Protection Rule, 76 Fed. Reg. 59805 (Sept. 27, 2011).

- *Fourth*, we agree with the Commission's proposal to interpret the term "online service" to mean "any service available over the Internet, or that connects to the Internet or a wide-area network."[10] ESA requested in its June 2010 Comments that the Commission confirm that the COPPA Rule does not apply to local communications, and the proposed interpretation does just that. Local communications networks are not "available over," and do not "connect[] to," the "Internet" because they are not part of the "the interconnected world-wide network of networks."[11] They also are clearly distinguishable from wide-area networks, which span large geographic areas that cover hundreds of miles or more.[12]

We are concerned, however, that certain other aspects of the proposed rule would create regulatory uncertainty that impedes video game operators' ability to maintain, much less broaden, the range of online entertainment options available to children. In general, ESA is concerned by the Commission's proposal to expand the definition of "personal information" to include several new classes of data and to potentially limit the ways in which operators can obtain parental consent.

In particular, ESA urges the Commission to further revise the proposed COPPA Rule in three key areas so that operators can continue to innovate and offer interactive online experiences to children in ways that meaningfully protect their privacy and security.

- *First*, ESA urges the Commission to refrain from expanding the definition of "personal information" to more broadly include "screen names" and "persistent identifiers."[13]

- *Second*, we encourage the Commission to retain existing parental consent mechanisms such as email plus, and to encourage new, innovative mechanisms

[10] *Id.* at 59807.
[11] 15 U.S.C. § 6501(6).
[12] *See, e.g.*, Webster's II New College Dictionary (3d ed.) (defining a "Wide Area Network" or "WAN" as a "communications network that uses such devices as telephone lines, satellite dishes, or radio waves to span a larger geographic area than can be covered by a LAN," or "Local Area Network").
[13] Although ESA is concerned with any broadening of the definition of "personal information," we focus our comments here on two such classes of data — "screen names" and "persistent identifiers" — because these identifiers are integral to the online game space, where many parents purchase, download and install video games specifically because they want their children to be able to participate in the game's interactive services and features.

that are scalable and parent-friendly so that game operators have flexibility to deliver a wide range of video games, including free versions of such games, to children.

- *Third*, we ask that the Commission confirm that parental notice and consent requirements can be streamlined where the service offerings are provided jointly by multiple operators.

As our comments reflect, it is imperative that any revisions to the COPPA Rule neither upset the careful balance that currently exists between parental engagement and industry innovation, nor discourage an environment in which our industry — which produces rich, dynamic, educational and fun interactive game experiences that parents want their children to experience — can continue to expand the universe of online game offerings for children.

I. THE COMMISSION SHOULD NOT EXPAND THE DEFINITION OF "PERSONAL INFORMATION" TO MORE BROADLY CAPTURE SCREEN NAMES AND PERSISTENT IDENTIFIERS.

The Commission proposes to expand the definition of personal information to several new categories of data, and in so doing would subject a considerably broader set of operators to COPPA's requirements. To be clear, the video game industry understands and supports the important objectives COPPA promotes. Our industry is also, of course, one that has a keen interest in catering its entertainment offerings to children.

We believe that the marketplace explosion of dynamic, interactive content available to children, and children's robust participation in such offerings, demonstrates that our industry is ably meeting the demands of parents and children for rich entertainment experiences for children consistent with COPPA's objectives. Unfortunately, the proposed expansion of the "personal information" definition would severely impact game publishers' ability to make game offerings available to younger users. In the online game context, this impact is most readily

demonstrable with respect to the proposed broadening of when screen names and persistent identifiers are included in the definition of "personal information."

Accordingly, for the reasons explained below, we urge the Commission to refrain from expanding when screen names and persistent identifiers are treated as "personal information." If, however, some expansion to the definition of "personal information" is included in the final COPPA Rule, the Commission should, at a minimum, clearly and meaningfully limit the scenarios in which the newly added identifiers would trigger COPPA.

A. *The Proposed Rule Does Not Draw a Meaningful, Workable Line for When Screen Names or Persistent Identifiers Would Trigger COPPA Compliance.*

In the proposed COPPA Rule, the Commission identifies the concern driving its broader inclusion of screen names as the notion that these aliases "increasingly have become portable across multiple websites or online services, and permit the direct contact of a specific individual online" outside the specific site or service where the screen name was collected, and without any additional information.[14] Based on this concern, the proposed COPPA Rule presumes that screen names are equivalent to a real name or email address.

It also is clear, however, that the Commission appreciates that operators long have used screen names and persistent identifiers in myriad ways that do not implicate this stated concern, including to "aid the functionality and technical stability" of services and "to provide a good user experience."[15] Accordingly, the Commission proposes that collection of screen names and persistent identifiers would not trigger COPPA if such information "is used for functions other than or in addition to support for the internal operations of the Web site or online service," while simultaneously proposing to expand, somewhat, the definition of

---

[14] Children's Online Privacy Protection Rule, 76 Fed. Reg. 59810 (Sept. 27, 2011).
[15] *Id.* at 59809.

"support for the internal operations of the website or online service" to include "activities necessary to protect the security or integrity of the website or online service."[16]

ESA recognizes that the Commission's proposal is, on balance, intended to permit operators some flexibility in how screen names and persistent identifiers may be used absent parental consent. Unfortunately, the Commission's approach — which attempts to carve out exemptions from the premise that screen names and persistent identifiers constitute "personal information" — is bound to foster uncertainty and to chill innovation, especially given the rapid pace of technological change. The need to exempt a wide range of prevalent uses suggests that screen names and persistent identifiers are not themselves problematic, but rather that certain limited, transformative uses of those identifiers raise concerns. As such, any expansion of the "personal information" definition should be limited to these specific uses. If these uses cannot be clearly defined, then there is neither a compelling reason, nor a workable means, to expand the "personal information" definition beyond the current COPPA Rule.

Relying on a broad exemption to carve out commonly accepted uses of screen names and persistent identifiers also is problematic. Indeed, despite the Commission's thoughtful attempt to define the contours of the internal operations exemption, trying to parse the proposed COPPA Rule's guidance to determine which of the game industry's common uses of screen names and persistent identifiers would meet the internal operations exemption readily demonstrates the inherent ambiguity in the Commission's approach.

A few common examples of how the video game industry uses screen names reveal the difficulty in determining what is or is not "support for . . . internal operations." In explaining

[16] *Id.* at 59809–12.

the "internal operations" exception, the Commission elaborates that the exception would include uses "*within* a website or online service," but would exclude uses that are not "solely to maintain the technical functioning of the website or service."[17] A number of uses occur "within" a website or online service that may not be purely "technical" or "internal" in nature, such as ranking users in online leader boards, enabling live game play against other users, and publicly displaying in gamer profiles what games a user is playing, or what achievements the user has unlocked. Because these uses are not limited to back-end, technical functions and are not purely internal in nature, it is not clear whether these uses are permitted by the definition of "support" for "internal operations," or whether prior notice and parental consent are required.

Similarly, the Commission states that persistent identifiers do not trigger COPPA concerns when used "only to support the internal operations of a website or online service" as opposed to when they are used "to compile data on specific computer users" or for "amassing data on a child's online activities." Again, in the game context, there are scores of actual and potential uses that seemingly conform to both of these either/or conditions. It is not possible to perform many of the activities that the Commission explicitly permits under the definition of "support for the internal operations" — such as improving site navigation and maintaining user preferences — without gathering some data about the child's online activities over time. As such, if an online game service uses an identifier to "compile data," such as user achievements in a specific game or to improve the user experience over a number of game titles (e.g., totaling user experience points), does that "data compilation" alone trigger COPPA? Or, if that

---

[17] *Id*. at 59810.

identifier does not permit the user to communicate independently across multiple, otherwise unrelated sites and services, does that render the same amassing of that data mere "internal support?" We find no clear answer in the proposed COPPA Rule.

Screen or user names also may be employed "across multiple websites or online services" for the specific purpose of providing "support for internal operations." For example, a video game publisher might allow, or even require, a player to use the same screen name to sign in to online services that cover all of the publisher's games across multiple video game platforms — including different video game consoles, handhelds, and other mobile devices — so that the online service can function. This single screen name might allow the player to aggregate achievements and maintain user settings and preferences across the publisher's different video games (all activities that the Commission seems to characterize as support for internal operations), regardless of the platform on which the video game is played.

Additionally, screen names may serve a security function to enable the consumer to activate, access, or use an authenticated copy of the game software. Depending upon the publisher, this process may permit the consumer to download and/or play the game on multiple devices. Requiring the use of a single screen name across the publisher's games, regardless of the platform, would prevent two users who are playing the same game on different platforms from signing up for the online service using the same screen name, which could create technical and administrative challenges for the video game publisher's back-end systems and operations. Despite these clear operational benefits, it is unclear whether these

practices would require prior notice and parental consent in light of the Commission's ambiguous commentary.[18]

As these few examples amply demonstrate, the broader inclusion of screen names and persistent identifiers in the definition of personal information, even when coupled with a well-intentioned exemption for certain operational uses, would force prudent operators, including ESA's members, to carefully evaluate each use of screen names or persistent identifiers to determine on which side of this fuzzy line the proposed use falls. This regulatory uncertainty will undoubtedly shape both the types and range of functionality of games and services that are made available to children.

B. *The Proposed COPPA Rule Would Negatively Impact Game Offerings for Children Under 13*.

The video game industry has a vested interest in offering fun, enriching, interactive online games to children. That interest is reflected in the recent explosive growth in the market for online and mobile casual or "lite" (i.e., free to play) versions of games, some of which may be directed to children. These games rely on high numbers of users and sustained user engagement to succeed. Accordingly, retaining low cost barriers and minimal friction to entry is critical.

[18] Confusion also might result where screen names and persistent identifiers are used within a family of websites or online services. Such sharing, which is common across a number of different industries, has the primary purpose of helping support the functioning of the websites and services within the corporate family. For example, a parent company might create a central database of customers' personal information (1) to help ensure that this information remains accurate (e.g., where a user corrects an e-mail address on only one of the corporate websites); (2) to help protect this information from unauthorized access, loss, or misuse; (3) to apply user settings and preferences across the family of sites; and (4) to customize content and advertising within the sites. While we understand that the Commission intends to allow screen names and persistent identifiers to be used within a corporate family in at least some circumstances, this intention is not clear from either the text of the COPPA Rule or the Commission's commentary.

Ambiguity over the internal operations carve-out may prompt some prudent operators to conclude they should seek COPPA consent in situations where, in fact, it may not be necessary. However, an overbroad application of parental consent requirements has certain consequences. The business reality is that applying COPPA's parental consent requirements to the user sign-up process for activities that have minimal privacy implications both increases the cost of user acquisition[19] and radically increases user drop-off.[20] To date, the video game industry has been able to design game offerings for children by refraining from collecting "personal information" as defined under the current COPPA rule, relying instead on screen names and other persistent identifiers as proxies to enable interactivity and user customization.

For the video game industry, expanding COPPA's scope to more broadly reach these anonymous identifiers will incent operators in one of two directions. Operators who obtain verifiable parental consent in order to continue offering children engaging online experiences will actually increase risks to consumer privacy. As noted above, video game publishers and console and handheld manufacturers often collect screen names and persistent identifiers specifically to avoid the collection of other, more sensitive types of personal information, such as children's full names or e-mail addresses. However, the operator will need to collect additional, more sensitive personal information from the child (including the parent's online contact information and the name of the child or the parent) and from the child's parent (potentially including highly sensitive information, such as the parent's credit card number and security code, driver's license or Social Security number) in order to fulfill the consent

[19] Generally speaking, the cost of a customer support call, one method by which parental consent might be secured, ranges from $4-$5 per call. In online games where the desire is to yield a high numbers of users, that cost quickly sinks the profit and loss potential of the game, particularly for free-to-play games.

[20] By some estimates, requesting credit card information alone will decrease user conversion rates by over 66 percent.

requirement. To cover the substantial expense of implementing verifiable parental consent mechanisms, these operators also are likely to try to recover their costs by charging fees for game services that otherwise might be offered for free.

Of course, other game publishers are likely to conclude that the costs of offering games to children make the business model unworkable. To avoid this dilemma, some operators will avoid directing their games and services to children or age-gate games with interactive or customization features in order to maintain a bright line for COPPA compliance. Others might instead limit the functionality of the game or device to avoid collecting screen names or persistent identifiers where any of their intended uses might not be deemed “support for the internal operations of the Web site or online service.” For example, free mobile video game applications that collect age information, which often are “lite” versions of popular game titles, might disable any interactive functionality or customization that requires the creation of screen names, including multiplayer modes. This result would potentially affect all users, and not just children under 13, because few mobile app developers will be willing to develop what, in effect, amounts to two different versions of the same application — one where a screen name is collected, and another where it is not.

We appreciate that the Commission recognizes these potential risks, and has sought to address them through an “internal operations” exemption. However, as described above, we believe that the proposed approach creates regulatory uncertainty and therefore would yield the very results (namely, a reduction in free or low cost interactive entertainment options for children) that the Commission seeks to avoid. Under the current COPPA rule, game publishers and console makers have the necessary flexibility to offer online entertainment to children that

is interactive and customizable, while still protecting children's personal information. As a result, parents and children alike benefit. The uncertainty introduced by the proposed expansions of the "personal information" definition, however, will upset this balance and inevitably reduce the number of offerings and the extent of functionality available in games directed to children by publishers who take their COPPA obligations seriously.

C. *The Commission should not expand the definition of "personal information" to more broadly cover screen names and persistent identifiers.*

For the reasons outlined above, we believe that the current COPPA Rule strikes an effective balance and that no changes to the "personal information" definition to more broadly encompass screen names and persistent identifiers are necessary. Should the Commission identify a particular use of screen names or persistent identifiers that raises concerns equivalent to those presented by use of real names and email addresses, then any expansion of the "personal information" definition should be narrowly tailored to cover only that particular use, and leave operators free to continue the many beneficial uses of screen names and persistent identifiers made today. As a matter of clean construction, tying the broader inclusion of screen names and persistent identifiers to the narrow use motivating the change makes sense. Such an approach also is far less likely to stifle incentives to offer content to children, as screen names and persistent identifiers would presumably not trigger COPPA except in the narrowly defined circumstances where they function as equivalent to the forms of personal information currently covered by the Rule.

In addition, given the potentially increased significance of the definition of "support for the internal operations of the website or online service,"[21] the Commission should further revise that definition to more clearly encompass standard business needs and practices that do not implicate privacy concerns. Among others, an expanded definition should clearly account for the following uses:

- *Authenticating users, improving site navigation, maintaining user preferences, serving contextual advertisements, protecting against fraud or theft, providing or restricting access to the site or service, identifying users to each other, and recalling user settings.* ESA appreciates that each of these uses are mentioned in the commentary to the proposed COPPA Rule, and requests that the Commission confirm that the definition includes these uses when adopting any changes in its final rule.

- *Managing game play and user settings*. Although these uses may not relate to the "technical" functioning of the site or service and may not be limited to the operator's back-end systems, they should be included because they clearly enable the functioning of the Web site or online service.

- *Delivering first-party advertisements and creating personalized content or features*. These activities, which are analogous to serving contextual advertisements, also should be explicitly included in the definition.

- *Using analytics to improve site or service navigation and other product and service offerings*. Many companies use either their own or third-party analytics services to improve site or service navigation and other product and service offerings. The revised COPPA Rule should make clear that the collection of persistent identifiers for such purposes is permitted.

- *Market research and product development*. These activities are commonly accepted and present minimal privacy risks.

[21] ESA also encourages the Commission to consider whether other categories of "personal information" should be qualified by the "support for the internal operations of the Web site or online service" carve out. For example, it would be appropriate to limit the inclusion of online contact information, photograph, video, and audio files, and identifiers that link the activities of a child across different websites or online services to those circumstances where the information is not used for the support for the internal operations of the website or online service.

- *Providing product support and responding to user requests*. As drafted, the rule permits such activities, but only if they fall within existing exceptions to the parental consent requirement. As explained below, customer support representatives may need to retain the user's information in some circumstances, making these exceptions unavailable.

- *Responding to law enforcement inquiries, protecting users' safety, and protecting intellectual property rights*. ESA appreciates that the Commission has proposed to amend the definition to include activities that "protect the security or integrity of the Web site or online service," and that the Commission clarified that this language covers security threats, fraud, denial of service attacks, and user misbehavior. We believe that the expanded definition is intended to encompass these additional uses as well, but further clarity would be helpful.

In addition, should the Commission retain the proposed expansion of the definition of "personal information" in some form, it should balance that expansion with a parallel extension of the parental consent exceptions, such as the one-time contact exception. For example, the proposed expansion of the "personal information" definition could make it difficult for companies to respond to children's customer service inquiries using VoIP, online video conferencing, and similar online technologies given that customer service representatives typically retain copies of all call records for operational purposes, making the one-time contact exception unavailable. The Commission could avoid this issue by revising the one-time contact exception to require that the online contact information be deleted, unless it is retained for the support for the internal operations of the website or online service and is not used to re-contact the child. In addition, the Commission should either specify that children may submit a photograph, video, or audio file in connection with a contest under the one-time contact exception or add a new exception permitting such collection. Like the proposed addition of an

exception covering parental notice, the collection of such information for these limited purposes is "reasonable and should be encouraged."[22]

II. SCALABLE, PARENT-FRIENDLY CONSENT MECHANISMS ARE CRITICAL TO THE FUTURE GROWTH OF RESPONSIBLE WEBSITES AND ONLINE SERVICES DIRECTED TO CHILDREN.

ESA believes that the Commission can help expand the range of online services directed to children by providing businesses a broader range of cost-effective and streamlined options for obtaining verifiable parental consent. In our view, this is one of the most important improvements that could be made to the Rule. Accordingly, we are pleased that the Commission proposes to add three new parental consent methods to its non-exclusive list of recognized practices — "scan and send" forms, video conferencing consent, and parental verification based on checks against government databases.[23] These mechanisms are a step in the right direction in ensuring that operators have a wide range of scalable, parent-friendly consent mechanisms. But the Commission should recognize additional options within the Rule, particularly those that can be used on a large scale and that harness ubiquitous technologies. Indeed, by recognizing additional parental consent methods that are easy on parents, easy to implement, and easy to scale, the Commission will spur publishers to innovate with both the type and range of interactive features that game publishers offer in child-directed products and services. Toward that end, there are other methods under consideration that meet the statutory standard in an equally effective manner.

[22] Children's Online Privacy Protection Rule, 76 Fed. Reg. 59820 (Sept. 27, 2011).
[23] ESA appreciates that the Commission's proposed voluntary approval process for new parental consent mechanisms is not intended to require companies to seek pre-approval of new parental consent methods that they develop, and that other, innovative forms of parental consent will remain acceptable to the Commission so long as they are reasonably calculated (taking into consideration available technology) to ensure that the person providing consent is the child's parent. *Id.*

The statutory definition of "verifiable parental consent" explicitly requires that the Commission "take into consideration available technology."[24] There is unanimous agreement that no failsafe technology currently exists to authenticate an individual's identity online or to verify or authenticate that there is a parental or legal guardianship relationship between the person providing consent and the child. Given available technology, e-mail plus is a sufficiently reliable method for internal uses, and parental control-based and "electronic sign-and-send" methods are each reasonable efforts to ensure that a parent of a child receives notice of and consents to the operator's collection, use, and disclosure of the child's personal information.

A. E-mail Plus and the "Sliding Scale" Standard Should be Retained.

The Commission should reconsider its initial decision to eliminate email plus and the sliding scale standard. The sliding scale approach has proven helpful in enabling a limited, but important, range of online activities, while adequately protecting children's privacy and keeping parents informed. Eliminating these helpful standards — which a number of companies, including several major video game publishers, have relied on to build substantial infrastructures to ensure compliance — would make it harder, not easier, to offer children robust interactive game experiences. Based on our members' direct experience with email plus, we believe strongly that this method of obtaining parental consent continues to be a useful option that should not be retired.

The circumscribed use of email plus for internal situations provides essential flexibility in the COPPA Rule. For example, some of ESA's members rely on e-mail plus to collect a child's

[24] 15 U.S.C. § 6501(9).

postal address to send items related to birthday clubs and prizes.[25] E-mail plus also is used to enable children to draw and save pictures (in which the child could potentially include personal information) on child-directed websites and services that do not disclose such user-generated content to the public. In such circumstances, the burden of requiring operators to spend potentially hundreds of thousands of dollars to convert to and manage a new, more robust parental consent process and train customer service personnel far outweighs any speculative benefits that might be realized from abandoning e-mail plus, which remains one of the most universally accessible online technologies available. Some game publishers confronting those costs may conclude that it is simpler to age gate or remove certain interactive features rather than build an infrastructure for obtaining consent through more onerous methods.

The commentary to the proposed COPPA Rule suggests that widespread adoption of email plus has discouraged innovation in the development of new parental consent methods.[26] To the contrary, the record in this proceeding demonstrates that since the Commission last reviewed the COPPA Rule in 2005, operators have given much careful thought to how the process of obtaining parental consent could be improved and have developed a number of innovative methods that rely upon a variety of new technologies, including text messaging, scanners, video conferencing, parental controls, and on-screen signatures. The record suggests that some operators have delayed implementation of these systems due to the absence of clear

[25] *See* COPPA FAQ # 42, http://www.Commission.gov/privacy/coppafaqs.shtm (requiring operators to provide parents notice and obtain verifiable parental consent before collecting a child's mailing address in connection with a contest).

[26] To support its assertion that e-mail plus has stymied innovation in parental consent mechanisms, the Commission cites to comments filed by Privo, which runs one of the COPPA Safe Harbor Programs. Notably, however, Privo's argument was limited to parental consent methods for "internal uses"; its comments still support the retention of the e-mail plus method and the sliding scale approach. See Letter from Denise G. Tayloe, President and CEO, Privo, to Donald S. Clark, Office of the Secretary, Federal Trade Commission, at 4 (July 9, 2010) (stating "Should Email Plus be Eliminated? Absolutely not. The 'plus' should simply get better along a sliding scale use of risk.").

guidance from the Commission on how the statutory standard will be interpreted and applied, and not because of e-mail plus.

Retention of the e-mail plus method is particularly important given the proposed expansion of the definition of "personal information." These changes are likely to significantly increase the number of operators that will need to obtain parental consent. For many of these operators, e-mail plus will be appropriate. For example, the internal collection and use of Voice over Internet Protocol ("VoIP") identifiers and video chat user identifiers (neither of which are subject to a carve out for the support for internal operations) presents minimal privacy risks.

In addition, the elimination of the e-mail plus method could have the unintended consequence of requiring operators to collect additional, more sensitive personal information in order to verify the parent's identity. Many operators would prefer to avoid collecting this more sensitive personal information, such as credit card information, the last four digits of a parent's Social Security Number, or the parent's driver's license number, as may be required by some of the full consent mechanisms. For example, a significant and growing segment of our industry offers "free to play" online games, which demand a low-friction entry point and emphasize a broad range of features which can be enjoyed without payment. Collecting a credit card or a driver's license number in this context would invite suspicion that the game is not the free, casual experience that the publisher has promoted it as being. Consequently, requesting this highly sensitive personal information from the child's parent may dissuade some parents from allowing their kids to play a game that may require parental consent only because it allows the child to draw pictures that are saved internally on the operator's servers.

Although it is true that the concept of a "sliding-scale" approach for obtaining parental consent is not explicitly authorized in the COPPA statute, the statute clearly contemplates a range of parental consent mechanisms because it requires only that an operator's efforts to obtain parental consent be "reasonable."[27] The "reasonableness" standard is common throughout data privacy and security law, and the Commission has repeatedly concluded that what is "reasonable" will depend on the privacy and security risks associated not only with the type of data collected, but also the particular use of the data.[28] Although ESA agrees with the Commission that children's personal information is sensitive, we urge the Commission, consistent with its precedent, to also consider how such information is being used. The e-mail plus method for obtaining parental consent appropriately distinguishes between the risks associated with internal, as opposed to external, uses of the child's personal information.

Absent clear evidence that the e-mail plus method is being abused by operators or that children are circumventing this method more than any of the other approved parental consent methods, including mailed or faxed "sign-and-send" forms, there is no public benefit in forcing operators to bear the substantial financial, administrative, and technical costs associated with overhauling their global compliance systems to implement new parental consent processes for relatively minor internal uses. To the extent that the FTC is concerned that some companies may be using email plus for activities requiring full consent, it would be more appropriate to

[27] Moreover, the "sliding scale" standard has been in use for nearly a decade; if Congress thought that this flexibility strayed too far from its intent, it has had ample opportunity to revisit and amend the statute to clarify this point. Notably, it has not done so.

[28] Fed. Trade Comm., *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, at vii (Dec. 2010) (stating that "[b]ecause of the significant costs associated with access, staff believes that the extent of access should be proportional to both the sensitivity of the data and its intended use").

deal with that problem through stepped up FTC enforcement actions rather than denying those who use email plus appropriately continued access to this important compliance tool.

B. ESA Is Encouraged That the Commission Will Continue To Consider Parental Control-Based Consent Mechanisms.

ESA proposed in its earlier comments that the FTC recognize a new form of verifiable parental consent obtained through the use of game console parental controls. In our experience, parents have strong familiarity with the parental controls features of game consoles and how those interplay with the content and functionality of the games themselves. We think it makes sense to leverage a technology parents are already familiar with to offer parents COPPA-compliant parental consent options. Additionally, console parental controls, by their nature, are reasonably calculated to ensure that the person providing the consent is the parent. Children are unlikely to try to set the parental controls by themselves because they have no incentive to restrict the console's functionality. And once the parental controls are enabled, only the parental password, PIN, or password-protected parent account can control the settings for the console or handheld, which prevents a child from overriding the parental control settings.

Each of the current-generation console and handheld systems has some degree of privacy settings. Adding parental consent to these parental controls would be conceptually related and have the benefit of providing parents an easy "one stop shop" for addressing multiple settings at a time when the parent is most focused on privacy and safety issues.

ESA is pleased that the Commission remains open to the idea of allowing operators to use parental control-based methods to obtain verifiable parental consent before operators collect any personal information from the parent's child. As the industry with the most robust,

understandable parental control tools, video game console and handheld manufacturers look forward to continuing to develop parental consent mechanisms that provide parents meaningful opportunities to become engaged in their children's online activities, consistent with the statutory standard.

C. Electronic Sign-and-Send Mechanisms Are Consistent with the Statutory Standard.

In considering which new parental consent mechanisms to recognize, it is important for the Commission to look to technologies that scale well and that offer parents increased convenience while still meeting the "reasonably calculated" standard. We continue to believe that "electronic sign-and-send" can satisfy these requirements. The electronic sign-and-send method meets the statutory standard by taking into consideration the technical realities of available tablet, mobile device and other small-screen technologies that allow for the input of electronic signatures but that typically are not able to connect to computer peripherals such as printers, fax machines, and scanners.

Although the Commission expresses concern that there has been a proliferation of mobile devices among children, this access is no greater than children's access to computers and laptops that are connected to desktop printer, fax, and scanner machines.[29] Likewise, the "ease with which children could sign and return on screen consent" is no different than the ease with which children could print and sign a form, and return it via mail, fax, or an electronic scan. In short, electronic sign-and-send provides an equivalent assurance to the print, fax, and

[29] In expressing this concern, the Commission states that the mechanism may not "ensure that the person providing consent is the child's parent," quoting Section 312.5(b)(1) of the COPPA Rule. 76 Fed. Reg. 59804, 59818. Notably, however, no parental consent mechanism is required to meet this standard. Rather, the COPPA Rule states that the parental consent method "*must be reasonably calculated, in light of available technology,* to ensure that the person providing consent is the child's parent." 16 C.F.R. § 312.5(b)(1) (emphasis added).

scanner methods that the Commission has previously approved or is proposing to approve in the final COPPA Rule.

ESA appreciates that the Commission has not foreclosed the option of using an electronic sign-and-send method to obtain verifiable parental consent, and, consistent with the statutory standard, businesses may continue to develop parental consent methods that are reasonably calculated (taking into consideration available technology) to ensure that the person providing consent is the child's parent.

III. THE COMMISSION SHOULD CONFIRM THAT STREAMLINED PARENTAL NOTICE AND CONSENT PROCEDURES FOR JOINT ONLINE SERVICE OFFERINGS ARE CONSISTENT WITH COPPA.

Providing parental consent should never be a confusing process for parents. In the video game industry, we strive to make each compliance-related interaction with our customers as simple and clear as possible, including, of course, the COPPA parental consent process. Normally, this process is straightforward. However, there is one context in which obtaining parental consent can become unduly complicated: joint service offerings.

A. *Online Interactivity for Console and Handheld Games Often Requires the Cooperation of Joint Service Providers.*

In the video game environment, third-party publishers' video games run on top of a console or handheld maker's online platform. In some cases, the console maker may share personal information with the third-party software publisher in order to enable certain interactive features, such as in-game chat, online game play, and leaderboards, within a particular game that the parent has self-selected or approved for use on the game console. And in other cases, in connection with the child's use of a publisher's game, a console maker

may temporarily store on its servers a child's user-generated content, which may include personal information, before passing along that data to the game publisher.

Consequently, it is possible that *both* the maker of the Internet-enabled console or handheld and the video game publisher that builds online interactivity features into its game could, depending on the circumstances, be considered "operators" under the COPPA Rule. As such, both entities may feel compelled to obtain separate parental consent to offer functionality which, from the user's perspective, is an integrated and seamless experience. Though this may make sense from a compliance perspective, it makes no sense from a parent's perspective.

B. *Dual Consent Confuses Parents.*

Based on the experience of ESA and its members, parents who purchase for their children video games with interactive features want their children to be able to play the game and use these features "out of the box." Indeed, parents are confused when they are prompted to provide consent a second time to the video game publisher before the interactive features are enabled when they have already given consent for that same purpose to the platform operator (e.g., Xbox LIVE or PlayStation Network). Accordingly, requiring a separate consent for a single use of the same information in conjunction with a single joint-service offering does not further COPPA's goal of empowering parents.

The COPPA statute and the Commission's COPPA Rule currently permit platform operators and third parties who operate through these platforms to streamline the parental notice and consent process for the offering of joint services, which may depend upon the seamless exchange of data, including children's personal information, in order to offer the child

the requested service.[30] The COPPA statute permits one operator to provide notice and obtain parental consent on behalf of other operators who collect or maintain the child's personal information through the joint service, as long as, taking into consideration available technology, the operator reasonably ensures that the parent receives notice of the operators' collection, use, and disclosure practices and authorizes such practices before the information is collected from the parent's child.[31] Consistent with this statutory language, the Commission clarified in its 1999 COPPA Rule that one operator may provide notice on behalf of all other operators who maintain or collect personal information through the website or online service, as long as (1) the designated operator responds to all inquiries from parents and (2) the names of all the operators collecting or maintaining personal information from children through the website or online service are listed in a single privacy notice.[32]

However, because the proposed COPPA Rule deletes this "multiple operators" provision, clarification that operators may continue to rely on the statutory language to streamline notice and parental consent practices in the joint services context is particularly timely and critical. Some operators may be hesitant to continue relying on these innovative parental notice and consent solutions in the absence of more certainty that they will meet the requirements of the statute. Therefore, ESA encourages the Commission to confirm that such streamlined procedures are permitted under COPPA.

[30] Such streamlined procedures should be available for third-party geolocation service providers as well. For example, some video games that are played on mobile phones base certain achievements on a user's location if the user has affirmatively consented to sharing geolocation information with the game publisher.
[31] *See* 15 U.S.C. § 6501(9).
[32] 16 C.F.R. § 312.4(b)(2)(i).

C. Streamlined Consent Is Workable on a Game Console.

In the video games context, a console or handheld maker (regardless of whether this entity is itself an "operator," as that term is defined in the COPPA statute) might choose to serve as a clearinghouse that would provide baseline notice and obtain qualified parental consent on behalf of third-party publishers and application providers. In practice, this process might include any number of the following features: The console or handheld maker could choose to provide parents a baseline notice that makes it clear that the child's personal information will be disclosed to third-party game publishers and application providers who may collect, use, and disclose such information through the console or handheld in order to provide a joint or related service; the console or handheld maker could obtain verifiable parental consent for itself and those third-party video game publishers and application providers; the scope of the consent would be clearly defined and appropriately limited; in some cases, the parental consent obtained by the console or handheld maker might be effective across any of the console or handheld maker's related video game platforms and websites clearly referenced in the console or handheld maker's privacy policy; and any desire by third-party publishers to make any additional collection, use, or disclosure of the child's personal information could require the publisher to provide additional notice and to secure a secondary verifiable consent from the parent for such purposes.

D. Streamlined Consent Is Consistent with the COPPA Rule.

This approach is consistent with the parent's reasonable expectations about the scope of his or her parental consent, and it provides console and handheld makers flexibility to develop innovative video game services that work across their own platforms. It is worth

emphasizing that the effect of this approach would be only to streamline the COPPA Rule's notice and parental consent requirements by permitting a console or handheld maker to act as a clearinghouse for third-party publishers and application providers in providing notice and obtaining parental consent. It would have no effect on the other obligations that the COPPA Rule currently imposes on operators, including the requirement to stop collecting or to delete the child's personal information upon a parent's request.

Clarifying that such streamlined procedures are acceptable would ensure that the parent obtains clear and accurate notice in a manner that does not overwhelm or confuse the parent. Streamlined notice and consent requirements are consistent with parents' reasonable expectations, because in the majority of cases the parent of a young child will have purchased or installed the video game or app for the child, and therefore will have an opportunity to review the packaging or collateral to identify the publisher or developer and to determine whether the game or app contains interactive features.[33] The parent therefore will know who to contact in case he or she has questions about how the child's personal information is handled. Obtaining parental consent through one point of contact (i.e., the platform) also could discourage a child from falsifying his or her age in order to avoid having to obtain a parent's consent every time the child wants to play a new game or application. And this method promotes shorter, more simplified privacy notices that are consumer-friendly and can be accessed even on the small screen of a handheld or mobile device.

[33] Online-enabled games carry the notice "Online Interactions Not Rated by the ESRB." This notice warns parents about their child's possible exposure to chat (text, audio, video) or other types of user-generated content (e.g., maps, skins) that have not been considered in the ESRB rating assignment.

Given all these considerations, we urge the Commission not to revise the COPPA Rule in a manner that would preclude our industry from offering parents a streamlined consent procedure for joint service offerings.

CONCLUSION

ESA and its members remain committed to the goals of encouraging parental involvement and protecting children's privacy and safety online. We believe that the COPPA statute and the Commission's COPPA Rule are important tools for advancing these goals, and we look forward to continue working with the Commission as it finalizes its proposed rule.

Respectfully submitted,

/s/

Christian Genetski
Senior Vice-President and General Counsel
Entertainment Software Association