June 30, 2010

By Electronic Filing

Mr. Donald S. Clark
Office of the Secretary
Federal Trade Commission
Room H-135 (Annex E)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: COPPA Rule Review, P104503

Dear Secretary Clark:

The COPPA Rule Review presents the Commission with a key opportunity to promote the growth of new online services directed to children. The Entertainment Software Association ("ESA") encourages the FTC to seize this moment to make key adjustments to the COPPA Rule that could greatly enhance the diversity of online experiences available to children. The ESA represents nearly all of the major video game publishers in the United States. We are 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.

The ESA strongly supports COPPA's equally important goals of "enhanc[ing] parental involvement in a child's online activities in order to protect the privacy of children" while also "preserv[ing] the interactivity of children's experience on the Internet" and "children's access

to information in this rich and valuable medium."[1] The ESA and its member companies have long been committed to achieving these same goals for the video game industry. For example, in 1994, the ESA established the Entertainment Software Rating Board ("ESRB"). The ESRB is a non-profit, self-regulatory body that, among many other things, helps parents make informed decisions about the games their children play — whether online or offline — by assigning computer and video game content ratings and administering a COPPA safe harbor program.[2]

COPPA has proven to provide the Commission with reasonable flexibility over the last decade, and the Commission's COPPA Rule continues to be a useful means for addressing children's privacy online. However, some video game publishers have avoided offering websites and online services that are directed at children and have chosen to exclude children altogether from more general offerings because of regulatory uncertainty and compliance challenges. Therefore, we recommend that the Commission focus on measures that will encourage more — not less — participation by operators, children, and parents. With these goals in mind, there are four specific areas where ESA urges the Commission to change or clarify its COPPA Rule:

(1) ***Expand the List of Identified Parental Consent Methods to Offer More Consumer-Friendly, Effective, and Scalable Mechanisms***. The Commission should consider additional methods of verifiable parental consent that build upon parental controls, on-screen signatures, text messaging, and web-based forms in order to leverage existing technologies and provide a better experience for parents and children.

(2) ***Encourage the Use of Robust Automated Filtering Systems to Enable Operators to Offer Interactive Activities to Children in Privacy-Enhancing, Safe, and Cost-Effective Ways***. The Commission should clarify that operators can avoid the "collection" or "disclosure" of personal information by using robust, automated

[1] 144 Cong. Rec. S12787 (1998) (statement of Sen. Bryan).
[2] *See* Entertainment Software Rating Board, http://www.esrb.org/index-js.jsp (last visited June 28, 2010).

filtering systems. This is important to ensuring the continued availability and viability of chat and communications tools appropriate for younger audiences.

(3) ***Affirm that the COPPA Rule Does Not Apply to Local Communications.*** The scope of COPPA is limited to the Internet and does not apply to local communications. While we think this conclusion is clearly suggested by the COPPA Rule, it would be helpful if the Commission could issue guidance affirming this point.

(4) ***Continue to Educate Parents.*** The Commission has taken positive steps to educate parents about online safety issues. We encourage the Commission to launch new educational initiatives to improve parents' and children's understanding of COPPA and the COPPA Rule.

In addition, we urge the Commission to refrain from expanding the definition of "personal information" to include "persistent IP addresses," "online behavioral advertising," or "user or screen names." Broadening the definition of personal information to include these categories of information would result in negative and unintended consequences for consumers.

I. THE VIDEO GAME INDUSTRY PROMOTES PARENTAL INVOLVEMENT AND HELPS PROTECT CHILDREN'S PRIVACY AND SAFETY ONLINE.

The video game industry has undertaken a number of efforts to promote parental involvement and to protect children's privacy and safety online. Below, we summarize three of these efforts: (1) industry participation in COPPA safe harbor programs; (2) the industry's robust parental control offerings; and (3) the industry's educational initiatives.

A. COPPA Safe Harbor Programs Attract Broad Industry Participation.

Nearly two dozen game publishers participate in the FTC-approved COPPA safe harbor programs. Operating for nearly a decade, the ESRB's COPPA Safe Harbor Program is primarily directed to game publishers. But the industry's participation is not limited to the safe harbor

program which it operates. Some game publishers participate in other safe harbor programs. Taken together, this broad participation demonstrates an industry commitment to protect children's privacy on game-related websites.

B. The Video Game Industry's Robust Parental Controls Empower Parents to Protect Their Children's Privacy and Safety Online.

The video game industry's robust parental control tools are the most sophisticated available among all entertainment media. The Commission is well aware of the use of these parental controls to block games by ESRB rating. In these comments, however, we emphasize another dimension of the industry's parental control tools: features in game consoles that allow parents to manage and control how their children access the Internet and interact with others online.

Microsoft's Xbox 360 Console — The Xbox 360 system includes a number of features that allow parents to limit their children's online interactions, including through Xbox LIVE — the online service component to the Xbox 360 console. Using Xbox LIVE Family Settings, parents can create personal Xbox LIVE settings for a child that will apply to that child's account no matter which machine is used to access it. The console also can be configured to allow online gaming and communications only with approved friends and to require parental approval before new friends may be added. For example, in the "Privacy & Friends" menu of Xbox LIVE Family Settings, parents can manage with whom their child communicates (e.g., "everyone"/"friends only"/"blocked") and by what means (voice, text, and/or video).[3] In

[3] For further information about the Family Settings of the Xbox 360 console, please see Xbox, http://www.xbox.com/isyourfamilyset (last visited June 28, 2010).

addition, parents can block all sharing of their child's profile information, if desired. Content controls also help parents set limits on their children's access to member-generated content.

Sony's PlayStation 3 Console and PlayStation Portable — In addition to ratings enforcement, the Sony PlayStation 3 console and Sony PlayStation Portable handheld can be configured to block access to Internet browsing.[4] The PlayStation Network, which is the online service for the PlayStation 3 and the Sony PlayStation Portable, comes with additional parental controls. For example, when a parent creates a specific account for a child, the parent may block the child from chatting with other users.

Nintendo's Wii Console — Parents can restrict a variety of online communications using the parental control features available on Nintendo's Wii console. For example, the console's web browsing feature can be disabled, and it is possible to restrict the sending and receiving of messages both from games and within certain online games. Parents also can restrict the sharing of user-generated content in certain games and areas.[5]

Nintendo DSi Handheld System — The parental controls for the Nintendo DSi handheld similarly afford parents several options for managing their children's communications. Parents can limit the use of the local wireless chat feature (PictoChat), restrict access to the web browser, restrict the ability to exchange photos over a local wireless connection (including posting to Facebook), and block the exchange of certain user-generated content (e.g., where a

[4] *See* Playstation, http://us.playstation.com/ps3/features/ps_ps3_otherfeatures.html (last visited June 28, 2010).
[5] *See* Nintendo, http://www.nintendo.com/consumer/systems/wii/en_na/settingsParentalControls.jsp (last visited June 28, 2010).

game allows users to exchange game levels or artwork). Once parental controls are activated, the default for the Internet settings is "blocked."[6]

Taken together, the parental control features of the three current-generation console systems provide parents a significant degree of control over their children's online activities, including how their children interact with others online. The controls are easy-to-use, widely recognized by parents, and can be implemented in a matter of minutes. Indeed, many of the parental control settings allow parents granular control over their child's online activities, and the parental controls are a good complement to the protections under the COPPA Rule requirements.

C. *The Industry's Educational Initiatives Encourage Parental Engagement.*

Educating parents about online safety promotes parental involvement in children's online activities and, in so doing, furthers one of COPPA's key goals. The video game industry continually strives to find new ways to educate parents about online safety issues. In partnership with various organizations, including the national Parent Teacher Association ("PTA"), Wal-Mart, and Parenting.com, the ESRB has taken a number of steps to ensure that parents are informed about the rating system, parental controls, and online safety issues. For example, the ESRB and the PTA publish and distribute to parents a guide describing the ESRB's rating system and related parental control tools. In addition, the ESA is a strong supporter of Web Wise Kids, a national nonprofit organization that provides innovative tools to help children stay safe online.[7] We have partnered with many state Attorneys General and other state

[6] *See* Nintendo, http://www.nintendo.com/consumer/systems/dsi/en_na/settingsParentalControls.jsp (last visited June 28, 2010).
[7] *See* Web Wise Kids, http://www.webwisekids.org (last visited June 28, 2010).

officials across the country to create public service announcements for television, radio, online, billboards, and mall kiosks.

Individual members of the ESA also are actively involved in educating parents about online privacy and safety issues. For example, Microsoft has launched a "Get Game Smart" campaign to educate parents and children about making wise choices in their entertainment experiences, including online safety.[8] Among other resources, the GetGameSmart website provides detailed information on Microsoft's parental controls (called "Family Settings"), tips for parental involvement, and expert advice. And Nintendo dedicates a section of its website to "Info for Parents" that addresses parental controls in all Nintendo systems and provides educational materials in game manuals.[9]

Although not required or motivated by COPPA, these initiatives, when coupled with easy-to-use parental controls, are helping to engage parents and enhance many of the existing parental consent processes required under COPPA.

II. THE COMMISSION SHOULD EXPAND THE LIST OF IDENTIFIED PARENTAL CONSENT METHODS TO OFFER MORE CONSUMER-FRIENDLY, EFFECTIVE, AND SCALABLE MECHANISMS.

In conjunction with the video game industry's strong self-regulatory and voluntary efforts, the Commission's COPPA Rule continues to be a useful means to increase parental engagement and foster children's privacy online. The ESA supports the COPPA Rule's "sliding scale" approach of requiring one level of verifiable parental consent for internal uses and a higher level where a child's personal information will be disclosed to others. For some

[8] *See* Get Game Smart, http://www.getgamesmart.com/ (last visited June 28, 2010).

operators, one or more of the Commission's currently identified methods for obtaining verifiable parental consent have proven useful and efficient, and the ESA supports retaining all of the identified verifiable parental consent methods.

Unfortunately, however, the current methods do not work equally well for everyone. Many game publishers find that the currently identified methods for obtaining verifiable parental consent are cumbersome for parents and do not scale well for popular websites and online services. For example, the "print and send" method is impractical for video game consoles, handhelds, and mobile phones. While the "toll-free number" method can be a faster option, it is too expensive for many operators. Obtaining verifiable parental consent through a credit card transaction has the potential to scale easily, but cost, privacy considerations, and the potential to confuse parents can make it a difficult option to implement in the games context. Neither the digital certificates nor the "e-mail coupled with PIN or password" method have gained much traction.

Therefore, it would be helpful for the Commission to supplement its list of identified methods to include additional ones that scale for popular services, minimize the burden on parents, work in a mobile environment, allow for real-time access, and take advantage of existing technologies. Specifically, the ESA asks the Commission to identify at least four additional methods for obtaining verifiable parental consent for disclosures: (1) parental controls, (2) sign and send, (3) a text message transaction, and (4) a web-based opt-in list. In considering these and other verifiable parental consent methods, we ask the Commission to keep in mind COPPA's legislative history, which makes clear that the verifiable parental consent

[9] *See* Nintendo, http://www.nintendo.com/corp/parents.jsp (last visited June 28, 2010).

requirement "should be interpreted flexibly" and that "'[a]vailable technology can encompass other online and electronic methods of obtaining parental consent."[10]

A. Parental Controls

Parental controls have become increasingly robust and sophisticated since Congress enacted COPPA in 1998. As described above, all current-generation consoles include parental controls, and parental controls also are a feature of some online games and virtual worlds.[11] Therefore, it makes sense to consider how these tools could be harnessed for the related task of acquiring verifiable parental consent under the COPPA Rule.

Although the parental controls method could be structured in any number of ways and apply to a variety of platforms, one reasonable approach would be to allow the parent to provide parental consent as part of the process of setting up parental controls. When a parent configures the parental controls during set-up or registration, the parent also could be provided a direct notice that the operator would like to collect, use, and disclose personal information from the child and could be asked whether the parent wants to provide parental consent.

The parental control method is a "reasonable effort (taking into consideration available technology) . . . to ensure that a parent of a child receives notice . . . and authorizes the collection, use, and disclosure, as applicable, of personal information."[12] It ensures that the person providing consent is the child's parent because parental controls are managed by a

[10] 144 Cong. Rec. S12788 (1998) (statement of Sen. Bryan).
[11] *See, e.g.*, Club Penguin, https://secure.clubpenguin.com/manage_account/login.php (last visited June 28, 2010).
[12] 15 U.S.C. § 6501(9); *see also* 16 C.F.R. § 312.5 (stating that a parental consent method must be "reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent"); 64 Fed. Reg. 59888, 59901 (Nov. 3, 1999) ("In determining whether a particular method of obtaining consent is 'verifiable' under the COPPA, the Commission must consider: (1) whether the method ensures that it is the parent providing the consent; and (2) whether the method is a 'reasonable effort,' taking into consideration available technology.").

parent-created password or PIN system. Children are unlikely to try to set the parental controls by themselves because parents typically set up a new video game console in the home and children have no incentive to restrict their own functionality on the device. The parent could revoke consent at any time by changing the parental control settings. This method also is a reasonable effort, taking into consideration available technology, because each of the current-generation video game consoles already have built-in parental controls at no extra cost to the parent.

B. Sign and Send

Internet-enabled mobile devices — including mobile phones, tablet computers, and e-readers — increasingly include touch screens that allow a user to input data by touching or writing on the device's screen. The sign-and-send method for obtaining verifiable parental consent would take advantage of this new technology by enabling a parent to sign a parental consent form provided on the mobile device's screen and to send this form back to the operator using the device's Internet connection.

The sign-and-send method is the digital equivalent of the print-and-send method. However, it is even more robust than the print-and-send method in that, in order to ensure that the person providing consent is the child's parent, it couples the electronic signature with additional steps, such as a confirmatory message to the parent. The method also is a reasonable effort, taking into consideration available technology, because many new Internet-enabled devices, such as mobile phones, lack printing or faxing functionality.

C. Text Message Transaction

A text message transaction approach could be structured in a number of different ways, but essentially there would be a text message exchange with the parents providing their consent for particular activities and data collection. The text messaging transaction method ensures that the person providing consent is the child's parent, and the method is a reasonable effort, taking into consideration available technology. A child generally cannot obtain a mobile phone or wireless subscription without adult/parental involvement.[13] And, in some instances, parents can set up parental controls on phones that can further assist with this process. In addition, the parent will be alerted to a text message fee because wireless providers charge (either by the text or as part of a bundle) for text messaging services. Some wireless providers even itemize on the monthly bill the numbers to which text messages are sent for the entire family account, which provides the parent a reminder and an opportunity to revoke consent. And the method is a reasonable effort because text messaging has become a low-cost and widespread means of communicating and conducting commerce.

The text message transaction approach also is analogous both to the credit card transaction and the fax-and-send methods. Under the credit card and text message transaction methods, the parent provides consent by submitting a number that is tied to his or her personal account — either a credit card number or a mobile phone number. And in both scenarios, the parent receives a reminder of the consent on a monthly statement so that the parent has an opportunity to revoke the consent. The text message transaction method also is similar to the fax-and-send method, in that the parent uses a telecommunications device (i.e., a fax machine

[13] Indeed, a credit check is typically required to subscribe to mobile phone service.

or mobile phone) to send his or her electronic signature back to the operator nearly instantaneously.

D. Web-based Forms with a Central "Opt-in" List

Under this type of approach to obtaining verifiable parental consent, parents could self-verify on the Commission's website or the website of a trusted third party. Once the parent had verified his or her identity and the parent's relationship to the child, the parent would be issued a secure password or PIN that the parent could then provide to other operators as part of a web-based parental consent process.

The party that initially verifies the parent's identity could, for example, rely on the Commission's current credit card method for obtaining verifiable parental consent. A nominal fee in such circumstances would be much more reasonable because it is a one-time charge (as opposed to many small fees that accrue as the number of approved websites increases) that would be tied to an entity that the parent is much more likely to recognize on the credit card statement as being connected to the parental consent. This approach also has the advantage of significantly reducing the number of operators that would need to collect sensitive personal information from the parent, since operators who do not otherwise charge for their sites or services, such as free-to-play online game publishers, can rely on a web-based opt-in using a password or PIN instead of credit card information.

Using web-based forms in conjunction with a centralized parent opt-in list ensures that the person providing consent is the child's parent because the trusted third-party entity would verify the parent's identity. Once the parent has been verified and provides his or her secure password or PIN to operators of websites and online services as part of a web-based parental

consent process, the operator could then confirm the parent's consent by corroborating the password or PIN number with the trusted third-party entity.

The method also is a reasonable effort, taking into consideration available technology, because it builds upon existing methods of obtaining verifiable parental consent, such as the credit card transaction approach, but centralizes the process to minimize the burden on parents.

III. THE COMMISSION SHOULD ENCOURAGE THE USE OF ROBUST, AUTOMATED FILTERING SYSTEMS TO ENABLE OPERATORS TO OFFER INTERACTIVE ACTIVITIES TO CHILDREN IN PRIVACY-ENHANCING, SAFE, AND COST-EFFECTIVE WAYS.

Many game publishers have no need or desire to collect personal information from children under 13 years old, but would still like to create interactive experiences for these users in privacy-enhancing and safe ways. Currently, this is possible because of the definition of "collection," which states that an operator may enable children to participate in interactive activities, such as chat rooms and message boards, without triggering the "collection" definition, so long as "the operator deletes all individually identifiable information from postings by children before they are made public, and also deletes such information from the operator's records." [14]

However, there is some uncertainty about whether the use of automated filtering systems can avoid the collection and disclosure of children's personal information under COPPA. This has limited the ability of the marketplace to fully realize the benefits of filtering and the limited "collection" definition. The Commission should encourage further innovation

[14] 16 C.F.R. § 312.2 (2010).

and use of automated filtering systems by specifying that such systems meet the regulatory requirements, so long as the automated system, taken as a whole, is sufficiently robust.

One example of a model used in the industry today is a combination of adaptive white and grey lists coupled with some level of human engagement on the back end. The white list consists of a large assortment of permitted words; those words that are not on the list cannot be used and numbers are also excluded. These white lists are used in conjunction with grey lists, which consist of permitted words that are used in impermissible combinations (e.g., "truck you," "eat my banana," and "sofa king"). Human editors continually revise both the white and grey lists to keep pace with children's usage. When a child types text into the chat box, the filter examines the entire string *before* allowing it to be posted online. Typically, this automated filtering is coupled with some degree of human involvement on the back end, ranging from responding to "report abuse" issues to a team of human moderators that perform periodic spot checks.

The ESA does not endorse any particular approach or technological solution, and whether or not a filtering system is reasonably robust will depend on the circumstances. We do recommend that the Commission find that automated filtering systems, augmented by some degree of human involvement on the back end, are a legitimate means of preventing the disclosure of children's personal information.[15]

By encouraging the use of robust, automated filtering systems to prevent the collection or disclosure of children's personal information online, the Commission would encourage

[15] If the FTC were to require simultaneous human moderation *prior to* posting, such a requirement would effectively kill innovation in the marketplace for advanced automated systems. Only the very largest companies could afford the staffing necessary to effectively scan thousands of chat streams in real time.

greater innovation in automated systems and prompt more video game publishers to develop games that cater to the needs of children under 13 years old.

IV. THE COMMISSION SHOULD AFFIRM THAT THE COPPA RULE DOES NOT APPLY TO LOCAL COMMUNICATIONS.

By its statutory terms, COPPA's scope is explicitly limited to the "collection and use of personal information from and about children on the Internet."[16] This is true regardless of whether an operator collects, uses, or discloses the information through a "website" or an "online service."[17] Although the term "online service" is not defined, the legislative history of COPPA suggests that the terms "Internet," which encompasses "the interconnected world-wide network of networks,"[18] and "online" are intended to be used interchangeably:

> The **Internet** is quickly becoming an [sic] significant force in the lives of our children as it moves swiftly into homes and classrooms around the country. Currently more than 3 million children under the age of 18 are **online** and the number is expected to grow to 15 million by the turn of the century. I think all would agree that proficiency with the **Internet** is a critical and vital skill that will be necessary for academic achievement in the next century. The benefits of the **Internet** are extraordinary. . . . Users can conduct transactions such as stock trading, make travel arrangements, bank, and shop **online**. . . . Most people who use **online services** have positive experiences. The fact that deceptive acts may be committed on the **Internet**, is not a reason to avoid using the **service**. To tell the children to stop using the **Internet** would be like telling them to forgo attending college because students are sometimes victimized on campus. . . . The **Internet** offers

[16] *See* 15 U.S.C. § 6502 (2008) ("Regulation of unfair and deceptive acts and practices in connection with collection and use of personal information from and about children on the Internet").
[17] The fact that the term "operator" refers to a "website located on the Internet or an online service" does not broaden the scope of COPPA beyond Internet communications; rather, for the reasons identified above, the use of "Internet" in this definition is best interpreted as clarifying that websites located entirely offline, such as many Intranet websites, are not covered by COPPA.
[18] 15 U.S.C. § 6501 (2008).

> unlimited potential for assisting our child's growth and development.[19]

With this statutory framework in mind, the ESA requests that the Commission clarify that COPPA does not apply to local communications. Based on the language of the statute and its legislative history, the Commission lacks statutory authority to expand COPPA to local communications, where personal information may be transmitted from one device to another device (or multiple devices) in geographic proximity and where no personal information is transmitted over the interconnected world-wide network of networks.

For example, a tablet computer may offer a dual-connection mode that allows users to interact with one another through the Internet or through a local wireless feature. Communications transmitted via the local wireless mode, which enables device users within a limited range of each other (e.g., 100 feet) to chat locally, fall well outside COPPA's purview.[20]

The ESA appreciates that children's privacy is an important issue, regardless of the communications medium used. However, COPPA's notice, parental consent, and access structure is not well-suited for local communications because this structure was specifically designed for an Internet environment. Because local communications are not transmitted over the Internet, the device maker may have no way of knowing that an interactive feature that uses local communications has been activated and may have no way of determining a parent's contact information so that parental consent may be requested. Although local communications fall outside COPPA, it is worth noting that in many cases children's privacy and

[19] 144 Cong. Rec. S8482-83 (statement of Senator Bryan) (1998) (emphasis added).

[20] Even assuming, for the sake of argument, that online services do not require an Internet connection, surely Congress did not intend for the definition of "online service" to be read so broadly as to reach small, ad hoc networks of local users.

safety will still be protected. For example, if the tablet computer has parental controls, a parent may be able to deactivate the local wireless features.

Moreover, during the June 2010 FTC Roundtable, there was some discussion of whether offering interactive features on various devices would make the manufacturer an "operator" under the COPPA Rule. The fact that a game device or e-reader may enable Internet functionality is not and should not be determinative. Rather, the entity also must collect, use, or disclose a child's personal information for the Commission's COPPA Rule requirements to apply.[21] The Commission recognized this limitation when it first implemented COPPA in 1999, stating that "entities that merely provide access to the Internet, without . . . collecting information from children, would not be considered operators."[22]

V. THE COMMISSION SHOULD REFRAIN FROM EXPANDING THE DEFINITION OF "PERSONAL INFORMATION."

The ESA believes that any expansion of the definition of "personal information" to include persistent IP addresses, online behavioral advertising, or user or screen names is unnecessary to achieve the goals of COPPA. Such an expansion would have little or no benefit for children's safety but would cause significant harm to consumers.

A. Persistent IP Addresses

Deeming persistent IP addresses to be personal information would create a number of practical problems that would threaten the efficient functioning of the Internet.

[21] 16 U.S.C. § 6502(a)(1) (2008) ("It is unlawful for an operator . . . **to collect personal information from a child** in a manner that violates the regulations . . .") (emphasis added).
[22] *See* 64 Fed. Reg. 59888, 59891 (Nov. 3, 1999).

- Virtually every website that is directed to children would be subject to the COPPA Rule requirements, regardless of whether any additional information is collected, used, or disclosed, because the vast majority of browsers immediately and automatically collect a user's IP address and send this information to the website operator. It is unclear how a website could possibly obtain prior verifiable parental consent in this situation.
- The definition is unworkable because it can be difficult to distinguish between persistent and dynamic IP addresses.
- A video game publisher's efforts to enforce an age gate restriction would be frustrated because a publisher who wanted to avoid collecting IP addresses would have no way to prevent a child from back-buttoning or otherwise using the same computer to enter falsified age information.
- The ability of content owners to conduct online copyright enforcement could be frustrated. Without knowing whether a particular IP address related to a child or not, content owners may feel compelled to adopt the most conservative approach and treat all persistent IP addresses as potentially identifying a child. Doing so would trigger the need to obtain consent before transmitting the IP address information to an ISP for purposes of forwarding an infringement notice to the end user.

Importantly, the Commission correctly excluded IP addresses from the definition of personal information when it implemented the COPPA Rule in 1999.[23] As the Commission noted, IP address or similar identifiers must be associated with other individually identifiable

[23] 64 Fed. Reg. 59888, 59892 (Nov. 3, 1999).

personal information to be considered "personal information." We encourage the Commission to reach a similar conclusion here.

B. Online Behavioral Advertising

The issue of behavioral advertising is best addressed at the macro level rather than having a number of varied and potentially conflicting implementations. The Commission has already provided guidance regarding the use of children's personal information for behavioral advertising in the context of its *Online Behavioral Advertising Principles.*[24] Indeed, those guidelines deem data about children to be "sensitive data" for which companies should obtain affirmative express consent before using the data for behavioral advertising purposes. In addition, the advertising industry has developed self-regulatory principles in this area.[25] The Commission should continue to support self-regulation in this area.

C. User or Screen Names

The definition of personal information should not be expanded to user or screen names that are not otherwise combined with personal information. Like with the IP address issue, this is an issue the Commission has previously considered and rightly concluded that if a screen name is not associated with any individually identifiable information, it is not considered "personal information" under the Rule.[26] Many video game publishers use screen or user names, along with passwords, to allow children to participate on a website or online service

---

[24] *See* Fed. Trade Comm'n, *Staff Report: Self-Regulatory Principles For Online Behavioral Advertising* (Feb. 2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[25] American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau, and Council of Better Business Bureaus, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), *available at* http://www.the-dma.org/privacy/Self%20Regulatory%20Principles%20for%20Online%20Behavioral%20Advertising%2007-01-09.pdf

[26] *See* 64 Fed. Reg. 59888, 59892 (Nov. 3, 1999**).**

without disclosing any personal information. If the Commission were to define personal information to include user or screen names, it would become considerably more difficult, if not impossible, for publishers to provide children with meaningful interactive experiences online.

VI. THE COMMISSION SHOULD CONTINUE TO EDUCATE PARENTS ABOUT COPPA.

The ESA commends the Commission for undertaking a number of educational initiatives to inform parents and children about COPPA and the importance of protecting children's privacy and safety online.[27] As described above in Section I, the video game industry has undertaken numerous initiatives to educate parents about how to get involved in their children's online activities and to talk with their children about the importance of privacy and safety online. We believe that the single best way to achieve COPPA's goal of increased parental involvement is by making sure that parents are informed. Our experience with parental controls is that the better informed parents are about their choices, the more likely they are to get involved.

However, we cannot do it alone. Parents are likely to be more engaged if there is a greater national awareness of the COPPA Rule and how it works. We encourage the agency to consider launching additional outreach efforts to educate parents and children about COPPA and the COPPA Rule. The ESA is committed to working with the Commission in this endeavor.

VII. CONCLUSION

Without reservation, the ESA and its members are committed to the goals of encouraging parental involvement and protecting children's privacy and safety online. We believe that COPPA and the Commission's COPPA Rule are important tools for advancing these goals. As the Commission considers whether and how to update the COPPA Rule, we ask that the Commission focus on ways to leverage the tools, including parental controls and automatic filtering systems, that are already at parents' and operators' disposal. We also strongly support the expansion of the Commission's identified mechanisms for obtaining verifiable parental consent to include methods that scale well, leverage existing technologies, minimize the burden on parents, allow for access in real time, and work in the mobile environment. Such methods may inspire a host of new providers to enter the market for child-directed online games.

Respectfully submitted,

Kenneth L. Doroshow

Senior Vice President & General Counsel
Entertainment Software Association

[27] *See, e.g.*, Fed. Trade Comm'n, *Social Networking Sites: A Parent's Guide* (Sept. 2007), http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec13.shtm.