September 30, 2024

By Electronic Filing

Ms. Letitia James
Office of the New York State Attorney General
The Capitol
Albany, NY 12224-0341
childdataprotection@ag.ny.gov

RE: Child Data Protection Act, Advanced Notice of Proposed Rulemaking

To whom it may concern:

The Entertainment Software Association (ESA) submits these comments in connection with the preliminary efforts of the New York Office of the Attorney General (OAG) to implement regulations under the New York Child Data Protection Act (NYCDPA). ESA is the U.S. association for companies that publish computer and video games for video game consoles, handheld devices, personal computers, and the Internet. There are over 340 video game companies in the state of New York.

The video game industry is committed to ensuring that young players have safe and positive experiences online and continues to invest in developing solutions to promote privacy, safety, and appropriate parental involvement. To further these objectives, ESA urges the OAG to develop rules that provide operators with the flexibility to implement privacy protections, consent methods, and other measures that best suit their products and users. Specifically, ESA asks the OAG to:

- adopt COPPA's flexible approach to parental consent, avoid overly prescriptive informed consent requirements that could unduly burden or confuse users, and encourage the voluntary development and use of platform-based tools for informed notice and parental consent;

- provide a workable and clear standard for determining when a service is directed to minors that is consistent with COPPA and respects the constitutional rights of minors and adults;

- exclude de-identified data from regulation, which is consistent with the approach taken under state privacy laws; and

- align the NYCDPA's "support for internal business operations" exception to include activities permitted under COPPA.

Each of these points is discussed further in Sections I-IV below.

I. CONSUMERS BENEFIT FROM FLEXIBLE PARENTAL CONSENT AND INFORMED CONSENT MECHANISMS.

A foundation of data protection regulation is that context matters. Different approaches to obtaining parental consent and informed consent might be needed depending on a variety of circumstances, such as whether the consumer is interacting with a website accessed through a web browser, a mobile application accessed using a mobile phone, or a video game accessed using a console and television screen or handheld device. While some services require registration, others could be accessed without an account. These different experiences involve different technical capabilities and limitations, different screen sizes, different consumer inputs (such as a keyboard, touchscreen, or video game controller) — each of which can impact how notice and consent mechanisms function.

To effectively address this complexity, the federal Children's Online Privacy Protection Act (COPPA) and other minor protection laws apply a principles-based, flexible approach to parental consent for minors under 13 and informed consent. ESA requests that the OAG's approach to parental consent for minors under 13 be consistent with COPPA's verifiable parental consent (VPC) framework and avoid overly prescriptive informed consent requirements. The OAG also should allow (but not require) platforms to make available consent mechanisms that other operators utilizing that platform can use on a voluntary basis. These two measures would benefit consumers by making the consent process for parents and minors easy to understand and streamlined.

A. The OAG Should Enact Regulations That Are Consistent With the COPPA Statute's Flexible Framework for Obtaining Verifiable Parental Consent.

The COPPA statute authorizes any VPC mechanism that is a "reasonable effort (taking into consideration available technology)" to provide parents notice and obtain the parent's consent for current and anticipated collection, use, or disclosure of the child's personal information.[1] Consistent with this flexible framework, the Federal Trade Commission (FTC) has provided a list of verifiable parental consent methods in its COPPA Rule. The FTC has repeatedly recognized, however, that this list is not exhaustive and that any mechanism that satisfies the statutory standard is permissible.[2] In finalizing its last amendment to the COPPA Rule, the FTC explained that operators should "remain free to choose the [consent mechanisms] most appropriate to their individual business models."[3]

This flexible approach has been able to adapt over time to rapidly-changing technology, and has encouraged operators to deploy innovative approaches that are appropriate to the different types of information they collect and varied contexts in which such information is processed. For example, many developers of free-to-play games have declined to use currently pre-approved VPC methods that require collection of a driver's license, credit card transaction, or biometric information because such information is not otherwise needed to play the game. Instead, these developers have opted to use bespoke VPC methods more aligned with the

---

[1] 15 U.S.C. § 6501(9).

[2] *See* 78 Fed. Reg. 2972 (Jan. 17, 2013); 89 Fed. Reg. 2034 (Jan. 11, 2024).

[3] 78 Fed. Reg. 2972 (Jan. 17, 2013).

types of data the games process. Accordingly, the OAG should adopt a similarly flexible parental consent standard that encourages operators to develop innovative and scalable technical solutions that are tailored to the relevant service and context.

ESA members and operators across many varied industries have been successfully working within COPPA's VPC framework for over two decades, and many companies that operate services directed to minors under the age of 13 have already implemented a VPC method consistent with the COPPA statute. To ensure clarity and streamline verification for operators and parents alike, any regulations adopted by the OAG should recognize COPPA-compliant methods of obtaining VPC as being compliant for purposes of the NYCDPA as well. This approach also would help ensure consistency with numerous other state comprehensive consumer privacy laws, which recognize COPPA-compliant VPC methods as valid means of satisfying state law consent requirements for processing the personal data of minors under the age of 13.[4] Importantly, this result would benefit parents, who are already familiar with these types of consent mechanisms and are likely to be confused by a novel consent paradigm.

In contrast, rules that would require use of any particular technology or mechanism could unintentionally increase burden and cost to parents. Some emerging VPC mechanisms have not yet been widely adopted or proven broadly workable in the market for all contexts. And even for technologies that may currently be widely available, such mechanisms may become out-of-date over time as technology evolves or may be costly for smaller businesses to implement, ultimately increasing costs to consumers. Requiring use of a specific technology would thus needlessly limit operators' ability to innovate and develop VPC solutions that are easy to use by parents and consistent with rapidly-evolving technology. As noted above, an approach tracking the COPPA consent regime would avoid these concerns by enabling operators to rely on consent methods that are known to be workable and effective, and that can be adapted to the particular product or service being offered as it may evolve over time.

B. Regulations on Informed Consent for Teens Similarly Should Be Flexible and Avoid Unduly Burdening Users.

The OAG regulations should focus on ensuring that minors are provided the information they need to make an educated choice while minimizing disruption as they navigate online services. Thus, the regulations should not provide overly prescriptive guidance on when and where certain notices must be provided. To do so would be to disregard the wide variety of digital products and services available on the Internet and the unique functionalities of each platform and service. One-size-fits all guidance also would ignore how disclosures may be displayed differently based on the industry and type of service. For instance, disclosures may appear in different formats and in different locations on website browsers, mobile applications, video game consoles, and handheld devices. Thus, the regulations should allow operators of

[4] *See, e.g.*, Va. Code Ann. § 59.1-576(D) ("Controllers and processors that comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) shall be deemed compliant with any obligation to obtain parental consent under this chapter."). COPPA preempts state statutes that impose liability "in connection with an activity or action described in this chapter that is inconsistent with the treatment of those activities or actions under this section," so a state law that adopts an inconsistent parental consent standard could be vulnerable to preemption. *See* 15 U.S.C. § 6502(d).

digital products and services the flexibility to provide information in the manner that is most logical considering the nature of the service.

For example, the video game industry has created a streamlined approach to providing consumers, particularly teens, with the information necessary to make informed decisions about data processing. The Entertainment Software Ratings Board (ESRB) provides succinct indications of whether certain online features that require data collection and processing are available in a particular game. For instance, the ESRB indicates when a game involves the sharing of location information with other users, user-to-user interactions, and unrestricted access to the Internet via a browser or search engine.[5] This approach has created an essential, go-to source of information for all consumers, including parents and teens.

Regulation of methods for soliciting informed consent should be flexible to ensure that operators can provide information at the moment when it is most actionable and meaningful. For example, a video game player may be more likely to take the time to read and reflect on notices that come during natural breaks in gameplay rather than pop-ups that are displayed in the midst of an active game play session. Methods of soliciting informed consent also should avoid fatiguing the user with multiple notices and requests for consent. In some circumstances, requesting consent for multiple purposes in a single request can be more meaningful and understandable for the user.

Accordingly, the OAG's regulations should avoid developing prescriptive standards for the manner in which informed consent must be obtained and allow flexibility in the manner in which necessary and relevant information is presented.

C. The OAG's Regulations Should Encourage the Voluntary Development and Use of Innovative New Platform-Based Tools.

To promote further innovation in parental consent mechanisms, the OAG should allow operators of video game and other platforms to voluntarily implement platform-based consent mechanisms to streamline consent flows. ESA notes as a threshold matter that platform-based consent may not be appropriate or technically feasible for all platforms and should remain one compliance option among many.

Video game platforms are one point of entry for new players seeking to access gaming experiences. A user might be required to create an account for the game platform before they are able to access games, creating a convenient opportunity for a platform operator to provide required notices and secure consent. This would avoid a deluge of separate identical consents for each individual game, and could enable platforms to provide notice and secure consent on behalf of third-party publishers. For example, the platform could provide a baseline notice communicating that the user's personal information will be disclosed to third-party game publishers and application providers who may collect, use, and disclose such information through the platform in order to provide a joint or related service. The platform could then obtain informed consent or parental consent on behalf of itself and those third-party video game publishers and application providers. If a third-party publisher wanted to collect, use, or disclose the user's personal information in a manner not covered by the platform's disclosures, the

[5] *See* ESRB Ratings Guide, https://www.esrb.org/ratings-guide.

publisher could provide an additional notice and secure a separate consent from the minor or parent for such purposes.

Platform-based informed consent and parental consent could provide more clarity for minors and parents while remaining consistent with their expectations. When a minor or their parent purchases a video game console or subscription to an online gaming service, they expect that the minor will play games on that platform. In ESA members' experience from the COPPA context, parents are often confused when, after going through the consent flow *for the platform* and providing consent for their children to use interactive gaming features, they must separately provide consent to *the game publisher* for the particular game the child wants to play for that same purpose, and then again to *a different game publisher* when the child chooses to play a different game. Platform level consent would allow parents and minors to provide the necessary consent to use interactive gaming features in one streamlined setup process, while preserving the opportunity for supplemental notices and consents where necessary.

The ANPRM asks about what standards the OAG regulations should set for device communications or signals that a user is a minor or consents or refuses to consent to data processing. While well intentioned, such signals can create conflicts with existing age and consent mechanisms that can undermine, rather than enhance, consumer choices. As a result, regulations should acknowledge the limitations of these technologies and allow operators flexibility to determine how to apply them based on the particular context.

For example, where an operator has first-party knowledge of user age, the operator should be able to rely on that information and should not be required to act on third-party age signals that conflict. To decide otherwise would create confusion and increase the probability of a service receiving conflicting age signals. For example, when a parent creates an account for their child with the provider of a video game console or a video game publisher, they may provide the child's date of birth and (if that child is under 13) grant verifiable parental consent consistent with COPPA to the requested online collection, use, and disclosure of the child's personal information. If that child is subsequently playing the game but conflicting age information is provided through the age signal, this conflict makes the age signal unclear or ambiguous. As a result, an operator should not be required to comply with conflicting signals.[6] Instead, operators who collect first-party knowledge of user age should be able to rely on information they obtain directly from the user, or, if the user is a minor, the user's parent.

Because device communications or signals may transmit inaccurate information, the OAG regulations should clarify that there is no duty to investigate where there is conflicting age information. For example, the age signal may be inaccurate if a parent hands their phone or tablet to their child to play a game. A video game publisher could get one age signal when the game is played on one platform, and a different age signal when the same game is played on another platform. Importantly, the FTC has repeatedly reiterated that operators have no duty to investigate age,[7] so any regulations that would, in effect, create such a duty to resolve conflicts between the age a minor or their parent provides during account creation and the age indicated

[6] N.Y. Gen. Bus. Law § 899-ii(2) ("An operator shall not adhere to unclear or ambiguous communications or signals from a covered user's device…").

[7] *See, e.g.*, COPPA FAQ, at E.2; 76 Fed. Reg. 59806 (stating that operators need not "ferret through a host of circumstantial information to determine who may or may not be a child").

through the age signal (which could potentially change repeatedly over time) would be inconsistent with COPPA.[8]

Similar issues arise with respect to consent signals. For example, any technical specifications for a voluntary device communication or signal conveying consent must be carefully designed to ensure consistency with COPPA. An operator whose online service is directed to children under 13 or that has actual knowledge that it collects personal information online from minors younger than 13 must comply with COPPA.[9] Under COPPA, parents must provide "verifiable parental consent" before an operator may collect, use, or disclose online the personal information of minors under 13 years old, unless one of COPPA's various exceptions applies.[10] Importantly, COPPA requires that the parent's choices be "verifiable," and the COPPA statute and more than a decade of FTC guidance make clear that the standard is a high bar for ensuring that it is the child's parent or legal guardian who is exercising the choice.[11] When providing VPC under COPPA, a parent might choose to enable some information processing practices and disable others. Device communications or signals might be inconsistent with the parent's choices conveyed during the COPPA verifiable parental consent process. Accordingly, an operator who has obtained VPC from a parent should be permitted to disregard any consent signals, and instead process the child's personal information consistent with COPPA.

II. THE COPPA FRAMEWORK PROVIDES AN ADMINISTRABLE TEST FOR DETERMINING WHEN A SERVICE IS DIRECTED TO MINORS.

The stakes in developing a test that is administrable are high because failing to do so puts consumers' most fundamental free speech rights at risk. The FTC has recognized the difficulties of regulating the online activities of teens without unintentionally burdening the speech rights of adults.[12] Moreover, multiple courts across the country have found statutory schemes to be unconstitutional where they burden adult and minor access to constitutionally protected speech.[13] The process for determining whether a service is directed to minors should

---

[8] Notably, the FTC previously has encouraged the development of a technical specification to allow operators of child-directed sites and services to signal their status to third parties (such as social media plug-ins and ad networks) to facilitate COPPA compliance. Unlike such a signal, which can convey a static, reliable fact (i.e., that the particular website address is child-directed), purported age information (which varies over time and across individuals) cannot be reliably and effectively conveyed using a preference signal.

[9] *See* 15 U.S.C. § 6502(d) (preempting state laws that are "inconsistent with the treatment of those activities or actions under [COPPA]").

[10] *See id.* § 6502(a); 16 C.F.R. § 312.5.

[11] 15 U.S.C. §§ 6501(9), 6502(b); 16 C.F.R. § 312.5.

[12] *See* 76 Fed. Reg. 59805 (Sept. 27, 2011) ("[G]iven that adolescents are more likely than young children to spend a greater proportion of their time on Web sites and online services that also appeal to adults, the practical difficulties in expanding COPPA's reach to adolescents might unintentionally burden the right of adults to engage in online speech.").

[13] *See Free Speech Coal., Inc. v. Colmenero*, No. 1:23-CV-917-DAE, 2023 WL 5655712 at *11 (W.D. Tex. Aug. 31, 2023); *NetChoice, LLC v. Griffin*, No. 5:23-CV-05105, 2023 WL 5660155 at *21 (W.D. Ark. Aug. 31, 2023); *NetChoice, LLC v. Yost*, No. 2:24-CV-00047, 2024 WL 555904, at *14 (S.D. Ohio Feb. 12, 2024); *NetChoice, LLC v. Reyes*, No. 2:23-CV-00911-RJS-CMR, 2024 WL 4135626, at *8 (D. Utah Sept. 10, 2024). In explaining its support for the COPPA age cutoff to remain at 12 years old, the FTC also

enable operators to understand their compliance obligations and avoid burdening the protected speech of adults.

In the context of video games, for example, many of the games that are of interest to teens may similarly be of interest to adults. Features such as animated characters and activities such as racing are prevalent among games played by users of all ages. To avoid overreaching and regulating websites and services intended for and used by adults, the OAG should develop a clear and administrable test based on objective, observable evidence to determine whether services are primarily directed to minors.[14]

Specifically, the OAG should adopt regulations that include COPPA's multi-factor, totality-of-the-circumstances test for determining whether a service is directed to children.[15] This approach has several advantages:

- First, these factors focus on those aspects of a service that can be easily, accurately, objectively, and consistently assessed by operators. As a result, operators have more predictability in assessing whether their services are directed to minors and are in a better position to understand their compliance obligations.

- Second, these factors strike a balance between weighing competent and reliable empirical evidence of audience composition while not mandating operators to proactively measure the age of their audience. Any age verification or estimation requirements could be privacy invasive and encourage operators to collect more personal information than is otherwise necessary to provide a service.

- Third, applying the COPPA Rule's multi-factor test would avoid arbitrary and capricious results where a single factor might suggest an online service is directed to minors while many other factors do not. For example, it would be incorrect to conclude that because a service uses animated characters, it must be primarily directed to minors — all video games use animated characters, but some games that use animated characters have subject matter and themes that are mature and intended for adults. Similarly, a game that features exploration and world building may be a subject matter equally interesting to minors and adults alike. An analysis of the totality of the circumstances of the game is necessary in either scenario to determine whether the game is or is not primarily directed to minors.

---

acknowledged that "as children age, they have an increased constitutional right to access information and express themselves publicly." 76 Fed. Reg. 59805 (Sept. 27, 2011).

[14] In the absence of a clear test to determine how to distinguish between services directed to teens and adults, the NYCDPA may be void for vagueness. A law is unconstitutionally vague if it "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." *United States v. Williams*, 553 U.S. 285, 304 (2008). Absent clear regulations on which services are in scope, operators would not have fair notice of their obligations under the law and could be subject to arbitrary and inconsistent enforcement.

[15] *See* 16 CFR 312.2.

- Fourth, the existing multi-factor test appropriately focuses on factors that are within the operator's control. The majority of the factors in the COPPA Rule's test for child-directedness focus on choices made by the operator — subject matter, design choices, language directed to children, incentives or activities appealing to children, whether child models are featured, use of child celebrities, how the service is advertised, and evidence of intended audience, etc. Whether children in fact use the service is only one factor in the test (i.e., evidence of audience composition). The COPPA Rule's test strikes the right balance of imposing obligations on operators that are actively directing their services to minors, rather than focusing on services that happen to be appealing to minors.

Given that the COPPA Rule's test for child directedness is designed for services directed to minors under 13 and the NYCDPA covers all minors under 18, the OAG should take a modified approach by weighting certain criteria more heavily than others. In the context of video games, the presence of music, animated characters, or subject matter (e.g., world building) would not always conclusively distinguish services directed to minors from those directed to adults — particularly when distinguishing between services that are directed to teens as opposed to adults. The regulations could specify, however, that factors in the COPPA Rule's test such as audience demographics, advertising and marketing, and language be given greater weight in the totality-of-the-circumstances test of whether a service is directed to minors.

The regulations should also recognize that services should be deemed directed to minors only if they are *primarily* directed to minors, similar to the FTC's test for assessing whether a child-directed service is *primarily* directed to minors under 13.[16] This clarification would be particularly important in distinguishing services that are directed to a general audience from those that are primarily directed to minors. Consistent with the approach taken in the COPPA Rule, general audience services would not be deemed primarily directed to minors solely because minors access the services or the services appeal to minors, but rather the totality of the circumstances would need to demonstrate that minors are the primary audience of the services.[17]

III. THE OAG SHOULD EXCLUDE AGGREGATED AND DE-IDENTIFIED DATA FROM THE NYCDPA'S DEFINITION OF "PERSONAL DATA."

The OAG regulations' definition of "personal data" should exclude data that is aggregated or de-identified. Data that is aggregated or de-identified cannot reasonably be linked to a specific individual, and therefore is not subject to the concerns underlying the NYCDPA.[18]

---

[16] *See NetChoice, LLC v. Griffin*, No. 5:23-CV-05105, 2023 WL 5660155, at *14 (W.D. Ark. Aug. 31, 2023), finding that a similar statute was likely to be unconstitutionally vague because it referred to the "substantial" or "predominant" function of a service or application with no further explanation of how platforms are to determine which function is "predominant."

[17] 78 Fed. Reg. 12, 3984 (Jan. 17, 2013). *See also Computer & Commc'ns Indus. Ass'n v. Paxton,* No. 1:24-CV-849-RP, 2024 WL 4051786 (W.D. Tex. Aug. 30, 2024) (interpreting the term "primary" in a Texas state law regulating minors' use of social media and concluding that "'Primary' has a fairly ascertainable meaning: 'for the most part' or 'in the first place'").

[18] *See* S7695B Sponsor Memo, 2023 Leg. Sess., (Ny. 2024) (specifying that the statute is intended to protect "the privacy of children and young adults by restricting digital services from collecting or using the

This approach also would be consistent with other state consumer privacy laws, which generally exclude aggregated and de-identified information from the definition of personal data.[19]

The appropriate standard for determining whether data is aggregated or de-identified should be whether the operator can re-link the data to a specific individual in the normal course of business. This would avoid an overly narrow standard based on speculative possibilities of reidentification, instead placing the focus on operators' actual data management practices. It also would ensure consistency with COPPA, which treats data as "deleted" when it "is not maintained in retrievable form and cannot be retrieved in the normal course of business."[20]

Allowing operators to make unregulated use of aggregated and de-identified data also would benefit minors by permitting operators to undertake activities such as product development and safety in a privacy protective manner. For example, game developers should be able to use de-identified gameplay data from minors to develop future games for minors, or to create chat filters and anti-harassment systems that protect the privacy and safety of users, including minors, online. An overly broad definition of personal information that included de-identified data would create a strong disincentive to invest in creating content for minors, and would inadvertently discourage important efforts to protect minors online. Additionally, such a definition would remove the incentive to pursue data minimization through aggregation and de-identification, which could unintentionally increase the amount of identifiable data collected and held by operators.

IV. PERSONAL DATA IS ESSENTIAL TO SUPPORT INTERNAL BUSINESS OPERATIONS THAT PROMOTE SAFE AND ENJOYABLE EXPERIENCES FOR MINORS.

The ANPRM recognizes that there must be exceptions from consent requirements. These exceptions are critical to allowing operators to conduct processing that is necessary to promote an engaging and safe online environment for minors, consistent with the goals of the statute. Accordingly, the regulations should clarify the scope of the exception for processing to support internal business operations under § 899-ff(2)(b). Doing so would help add consistency with COPPA and help mitigate the risk of federal preemption.[21]

A. The OAG's Regulations Should Clarify That Reasonable Processing Activities That Are Consistent With User Expectations Are Permissible.

The exception to the NYCDPA's consent requirements for processing that is "strictly necessary" recognizes that there are important situations where requiring operators to secure consent would limit their ability to provide online experiences without producing meaningful benefits for consumer privacy. The OAG's regulations should preserve this balance by allowing

---

personal data of users they know are under the age of 18 without consent, and prohibiting or requiring safeguards for the sale or disclosure of the personal data of users they know are under the age of 18").

[19] *See, e.g.*, Cal. Civ. Code § 1798.140(v)(3).

[20] *See* 16 C.F.R. § 312.2.

[21] *See* 15 U.S.C. § 6502(d) ("No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter that is inconsistent with the treatment of those activities or actions under this section.").

reasonable processing activities consistent with user expectations, while avoiding an overly narrow interpretation that might inadvertently result in fewer safe, age-appropriate online experiences for minors. Specifically, the OAG should recognize a multi-factor test for considering whether processing is "strictly necessary," considering the following factors:

- **Whether the function is inherent to the service**. Rather than taking a narrow view of what may be strictly necessary for the specific functionality of a website or service, the regulations should consider what is "strictly necessary" in light of the nature of the service as a whole so that functions inherent to the service are permissible.[22] For example, personalization is "strictly necessary" for a service that allows minors to access age-appropriate games, videos, and other content because the purpose of the service is to provide engaging, age-appropriate content. For instance, if a minor who is playing an educational game is struggling with reading but excelling at math, personalization allows the game operator to help the minor build their reading skills. In these examples, personalization is "strictly necessary" to achieve the broader goal of the service.

- **Reasonable user expectations**. Activities that are in line with a user's reasonable expectations when using the service should fall within the "strictly necessary" definition. For example, a user of a video game service would reasonably expect that their personal data might be processed for purposes of chat moderation to protect against bullying and harassment. If the use of personal data is within the user's reasonable expectation, there should be no need to obtain specific, informed consent to such processing.

- **Technical Support**. The OAG regulations should affirm that processing in connection with routine or incident-specific technical support activities is exempt from the consent requirement. Support teams responsible for investigating technical issues affecting a game or platform may need to access system components including databases and servers and incidentally process their contents, which may include personal information from minors. Additionally, it may be necessary in some cases for support teams to engage third parties to provide technical support and assistance, and to provide those third parties with access to relevant system components and the personal data associated with them. These processing activities are part and parcel of maintaining the functionality of video games and other services, and are clearly "strictly necessary" to "identifying and repairing technical errors that impair existing or intended functionality," one of the key purposes defined in GBL § 899-ff(2).

- **First-party processing**. The OAG regulations should recognize a distinction between first party processing, which may be strictly necessary, and third-party disclosures, which may not always be strictly necessary. First-party processing activities are generally lower risk to the minor, as recognized by the FTC in creating the support for internal operations exemption to the verifiable parental

[22] Notably, COPPA also recognizes that certain functionality may be so inherent to the service such that if a parent refuses to consent to such processing, the operator may deny service to the child. *See* 16 C.F.R. § 312.6(c).

consent requirement.[23] Activities such as "payment and delivery functions, spam protection, optimization, statistical reporting, or de-bugging"[24] are all first-party processing (including when performed by data processors) that pose low risks to minors and should be considered strictly necessary to provide a service.

- **Promoting access to online experiences for minors**. When COPPA was introduced in 1998, Congress recognized that "the Internet offers unlimited potential for assisting [a] child's growth and development" and that restricting children from the Internet was not the appropriate response to the potential risks posed to children.[25] Here, the OAG should avoid an unnecessarily narrow interpretation of "strictly necessary" that could have the unintended consequence of reducing age-appropriate experiences available to minors online. For example, an interpretation of "strictly necessary" that forecloses use of minors' personal data for purposes of product improvement and product development may lead operators to stop maintaining, or developing altogether, services designed for minors. The OAG should encourage the development of safe, age-appropriate experiences for minors by allowing operators to use minors' personal data for product improvement and development.

Clarifying that these processing activities are permitted by the exceptions to the NYCDPA will promote positive online experiences while mitigating risk of preemption by COPPA.

B. The OAG's Regulations Should Explicitly Recognize All Of The Activities Permitted Under COPPA's VPC Exceptions As "Internal Business Operations."

In addition to the multi-factor test described above for determining whether processing is "strictly necessary," the OAG's regulations should explicitly recognize all of the activities permitted under COPPA's VPC exceptions as "internal business operations." For example, the regulations should clarify that any processing to provide support for internal operations that is permissible under COPPA is also permissible under the NYCDPA's exception for processing for internal business operations. Specifically, adopting the support for internal operations exception from the COPPA Rule would cover processing for the following purposes: (i) maintaining or analyzing the functioning of the website or online service; (ii) performing network communications; (iii) authenticating users and personalizing the content of the website or online service; (iv) serving contextual advertising on the website or online service or capping the frequency of advertising; (v) protecting the security or integrity of the user, website, or online service; (vi) ensuring legal or regulatory compliance; and (v) fulfilling a specific request from a minor.

Under COPPA, operators may carry out processing to support internal operations while satisfying privacy-related obligations to minors under 13. Clarity that these same data processing activities are subject to the exemption for processing personal data of minors 13 and older would be beneficial to promote these processing activities that benefit consumers. In promulgating this exception to the COPPA Rule, the FTC recognized that these operations "are

[23] *See* 16 C.F.R. § 321.5(c)(7).

[24] 78 Fed. Reg. 3981 (Jan. 17, 2013).

[25] *See* 144 Cong. Rec. S8482 (daily ed. July 17, 1998) (statement of Sen. Bryan).

fundamental to the smooth functioning of the Internet, the quality of the site or service, and the individual user's experience."[26] The activities permitted under COPPA's support for internal operations exception are instrumental in the video game industry for operators to improve their services and offer an engaging experience that is personalized to the user and allows them to seamlessly build upon their progress in a game.

In particular, the regulations should clarify that trust and safety functions, such as those commonly employed in the video game industry, are within the scope of the NYCDPA's exception for internal business operations. In the video game industry, preventing fraud and cheating by bad actors is essential to ensure fair play and an enjoyable experience for users. Operators rely on personal data of users to identify bad actors and to train their systems to detect cheat behavior in the future. The regulations should make clear that this processing is permitted under the NYCDPA exception for internal business operations by adopting an explicit exemption for trust and safety and anti-cheating.

In addition, the regulations should clarify that processing that is strictly necessary to improve products and services is an "internal business operation" permitted under the NYCDPA, and that informed consent is not needed for such processing. Video game operators rely on the personal data of users to develop and improve the gameplay experience, and restricting their ability to process personal data of minors for this purpose will hamper these efforts, particularly for games that are primarily directed to minors. Recognizing product improvement as an "internal business operation" permitted under the NYCDPA would also be consistent with COPPA's support for internal operations exception.[27]

* * *

ESA and its members remain steadfastly committed to providing minors with meaningful online experiences in a safe and privacy-protective manner. We believe that this rulemaking presents an important opportunity for the OAG to ensure that the NYCDPA is implemented in a manner that advances these goals.

Sincerely,

Maya A. McKenzie
Senior Counsel, Tech Policy
Entertainment Software Association

---

[26] 78 Fed. Reg. 12, 3998 (Jan. 17, 2023).

[27] 89 Fed. Reg. 8, 2046 (Jan. 11, 2024) ("Other proposed additions [to the exception]—such as personalization, product improvement, and fraud prevention—are already covered [under the COPPA Rule].").