Thank you for the opportunity to provide feedback on the Advanced Notice of Proposed Rulemaking. The Software & Information Industry Association (SIIA) is the principal trade association for the information industry. From digital platforms and global financial networks to education technology providers and B2B media companies – SIIA represents the businesses and organizations that make the world work.

The intent of the *New York Child Data Protection Act* is to protect the privacy of children and young adults, and restrict digital tools from collecting personal data of users they know are under the age of 18 without consent, as well as prohibiting or requiring safeguards for the disclosure of the personal data of users they know are under the age of 18.[1] In this vein, our comments are driven by a recognition that kids deserve access to information and the virtual tools critical in keeping them connected and engrained in their communities – without fear of being exploited. Through a careful approach that incorporates lessons from past successes at protecting children online, we believe policymakers have the opportunity to prioritize the privacy and safety of kids while empowering parents to be active participants in how their child operates online.

Our responses to select questions for public comment follow:

**Primarily directed to minors**

**Question 1: The Child Data Protection Act applies where either operators have actual knowledge that a given user is a minor, or the operators' websites or online services are "primarily directed to minors" (GBL section 899-ee(1)). What factors should OAG regulations assess when determining if a website or online service is primarily directed to minors?**

For this part of Question 1, we provide feedback relating to the use of a website or online service in an educational setting.

Data is an important tool in the educational system's toolbox to ensure educational equity, funding, and student success. Without clarification from the legislature or the Office of the Attorney General's (OAG's) office, the CDPA will restrict New York's educational systems ability to collect, use, and protect student data. Specifically, we are concerned about the lack of guidance in how the CDPA will interact with New York's existing Education Law § 2D, which was passed a decade ago to protect student personally identifiable information from unauthorized disclosure. New York's education leaders and their partners have worked to protect student data under this law for the better part of a decade. However, the conflicts in the laws may unintentionally harm a school's ability to complete the important task of educating the youngest

[1] NY State Senate Bill 2023-S7695B (nysenate.gov).

New Yorkers.

We recommend that the OAG clarify that technology products used under contract with a school and that collect data subject to Education Law § 2D do not meet the threshold of being "primarily targeted to minors" and that providers of such technology products are not considered "processors" when under contract with a school. These products, for example, help teachers take attendance, send homework reminders, provide access to classroom curriculum, help students communicate with their teachers, and more. While these products do collect information from minors, this data is required to be protected by existing student privacy laws and is intended to be controlled by the schools. The customers of these products are not minors, but are schools, school districts, regional boards of cooperative education services, and state education agencies. The providers of these products are already subject to various requirements under Education Law § 2D, including requirements on contracts with educational agencies. We urge the OAG to clarify this in the upcoming rulemaking.

- **At present, the federal Children's Online Privacy Protection Act's enacting regulations assess whether a website or online service is "directed to children" under 13 based on the following non-exclusive factors: "subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the Web site or online service, as well as whether advertising promoting or appearing on the Web site or online service is directed to children... [and] consider competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience" (16 CFR section 312.2). Should OAG's assess a different set of factors when assessing what is attractive to minors under the age of 13? Why or why not?**

We strongly recommend that the OAG regulations remain consistent with the multi-factor, totality-of-the-circumstances test in the COPPA Rule when determining which services are primarily directed to minors under the age of 13. The COPPA Rule provides an established precedent that has proven workable for regulators and operators alike for decades. The OAG has also already enjoyed significant successes in previous enforcement efforts undertaken within this framework. Past successes include enforcement actions brought against both Mattel and Hasbro in 2016 – described by the OAG as "Operation Child Tracker."[2] Were the OAG to deviate from this precedent, it would create unnecessary confusion for both experienced regulators and operators, and without any clear corresponding privacy benefit to young people.

- **What other laws, regulations, or industry standards exist that contemplate whether material may be targeted towards minors? Do they impose restrictions on**

[2] A.G. Schneiderman Announces Results Of "Operation Child Tracker," Ending Illegal Online Tracking Of Children At Some Of Nation's Most Popular Kids' Websites (ny.gov).

**targeting towards minors of any age, or do they apply only to certain ages or age groups? On what are they based? How effective have they been at capturing the empirical behavior of minors?**

We recognize the challenge associated with determining which websites and online services are primarily directed to minors, when older teens and adults may have identical interests. Compounding this challenge, courts have found statutory schemes to be unconstitutional when they would burden adult and minor access to constitutionally protected speech.[3] To avoid overreaching and regulating websites and services intended for and used primarily 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, which ensures that only websites and services primarily directed to minors are in scope.

As part of this, we suggest that the OAG continue to leverage the COPPA Rule's multi-factor, totality-of-the-circumstances test and child-directed factors, but could place more weight on factors such as intended audience, component and reliable empirical evidence regarding audience demographics, advertisements and marketing, and language used by the service which are more likely to help differentiate between a service appealing to teens instead of adults. In contrast, factors such as subject matter, visual and audio design, and age of models could be given less weight as these factors are less likely to be different for teen and adult directed services.

**Question 2: The Child Data Protection Act's obligations include website or online services, "or portions thereof," that are primarily directed to minors. Should OAG regulations distinguish portions created by an operator and portions created by users of the website or online service? If so, how?**

While we recognize the interest in distinguishing among portions of a website or online service, in practice this will be extremely difficult to implement and we are concerned will disincentivize operators to create and offer age-appropriate content. Notably, this interpretation is also inconsistent with the COPPA Rule's totality-of-the-circumstances test. There are two fundamentally practical challenges with distinguishing those portions of a website that are directed to minors: 1) providing for workable user experiences and 2) avoiding perverse incentives to actually mothball positive content directed at minors.

First, some portions of websites are not a naturally distinct experience for minors and adults, even if minors, like adults, may find this content engaging. A minor's account is thus distinct from

[3] *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). In explaining its support for the COPPA age cutoff to remain at 12 years old, the FTC also acknowledged that "as children age, they have an increased constitutional right to access information and express themselves publicly. " 76 Fed. Reg. 59804, 59805 (Sept. 27, 2011).

a television or music station directed to minors. This is because it would be quite cumbersome for all users — many of whom engage with a variety of content genres regardless of their age — to require them to consent to each such station separately.

Second, it is critical to avoid disincentivizing age-appropriate content by treating age-appropriate content as a distinct portion of a service. Many entities would simply choose to remove age-appropriate content for minors if offering such content otherwise imposes the compliance requirements of the CDPA on the entire service.

## Personal data

**Question 1: How should OAG regulations concerning the definition of personal data account for anonymized or deidentified data that could potentially still be re-linked to a specific individual (GBL section 899-ee(4))?**

Consistent with state consumer privacy laws, we recommend that the OAG regulations exclude deidentified data from the definition of "personal data." Similarly, the regulations should adopt recognized standards for deidentified data to avoid confusion and conflicting understandings around reidentification. In line with emerging norms in U.S. privacy law, we recommend that this standard should be whether this data can be reasonably linked to a specific identified or identifiable individual in the ordinary course of business.[4] Deidentification is a privacy-protective tool, and it is critical to establish clear guidelines that avoid disincentivizing operators from undertaking productive activities that actually safeguard consumer data.

## Sale

**Question 1: The CDPA's definition of "sell" includes sharing personal data for "monetary or other valuable consideration" (GBL section 899-ee(7)). Are there examples of ways operators may share personal data that do not constitute a sale that should be explicitly noted in OAG regulations?**

We recommend that the regulations align the definition of sale with how that term is used in existing privacy laws. As an example, the definition of "sale of personal data" in Connecticut's Data Privacy Act, which includes examples of how operators may share personal data that does not constitute a sale, serves as a good reference point and one that has the benefit of practice.[5]

---

[4] *See, e.g.*, Cal. Civ. Code § 1798.149(v)(3); Colo. Rev. Stat. § 6-1-1303(170).

[5] "'Sale of personal data' means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. 'Sale of personal data' does not include (A) the disclosure of personal data to a processor that processes the personal data on behalf of the controller, (B) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer, (C) the disclosure or transfer of personal

The OAG regulations should ensure that the definition of "sell" does not preclude an operator from completing a transaction where personal data is exchanged for monetary or other valuable consideration like a photobook. The OAG should consider exceptions offered in other states such as Colorado. The Colorado Privacy Act includes an exception that allows an operator to "provide a product or a service specifically requested by a consumer or the parent or guardian of a child, perform a contract to which the consumer is a party, or take steps at the request of the consumer prior to entering into a contract[6]."

## Permissible processing

**Question 1: What factors should OAG consider in defining what processing is "strictly necessary" to be permissible without requiring specific consent? N.Y. GBL sections 899-ff(1)(b), 899-ff(2).**

It is in the interest of minors — particularly their ability to access information and educational resources online while maintaining age-appropriate content — that the OAG avoids overbroad consent requirements within the "strictly necessary" exception. As such, data processing that is consistent with the expectations of consumers should fall within the exception in order for it to be functionally useful. If this exception does not permit such processing, the exception is unlikely to achieve its intended purpose: protecting minors by enabling operators to curate their experiences online and eliminate inappropriate or offensive content.

**Question 3: The CDPA permits processing for "internal business operations." Are there examples of permissible processing pursuant to internal business operations that should be explicitly noted in OAG's regulations? GBL section 899-ff(2)(b).**

We believe the definition of "internal business operations" should mirror COPPA's internal operations exception outlined in its 2013 Rule. The U.S. Congress is currently considering bipartisan proposals to add this language to the underlying statute. Incorporating similar language into the OAG's regulations would provide consistency for practitioners.

---

data to an affiliate of the controller, (D) the disclosure of personal data where the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party, (E) the disclosure of personal data that the consumer (i) intentionally made available to the general public via a channel of mass media, and (ii) did not restrict to a specific audience, or (F) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction, or a proposed merger, acquisition, bankruptcy or other transaction, in which the third party assumes control of all or part of the controller's assets. *Connecticut Data Privacy Act*, § (1)(26)."

[6] Colo. Rev. Stat. § 6-1-1304(VIII).

## Informed consent

**Question 1: The CDPA permits teenagers (minors between the ages of 13 and 17) to provide informed consent to processing on their own behalf (GBL section 899-ff(3)). What obligations should OAG regulations specify concerning the manner in which operators may request such informed consent?**

We recommend the OAG to ensure regulations for both CDPA and SAFE for Kids Act do not conflict and allow for flexibility in terms of how consent is obtained. Entities will have significant challenges complying to both laws with conflicting requirements. Instead, we believe that as long as consent is properly informed, applications should be able to leverage a variety of methods and evolving technologies in order to obtain these consents.

**Question 2: What standards should OAG regulations set for acceptable device communications or signals that a user is a minor or consents or refuses to consent to data processing? GBL sections 899-ff, 899-ii.**

In creating standards for browser or device signals concerning a user's age or minor status, it is important to recognize that these tools may still be ineffective in some circumstances. For example, at a high level, these signals are incapable of differentiating when minors are using adult accounts to access social media platforms. Furthermore, especially if age data is sourced from a variety of third parties, conflicting or unreliable signals could result.

Any regulation must account for the fact that this technology is relatively new. The OAG regulations should include appropriate safeguards and requirements to ensure technologies used in this space are secure, particularly since they will be used to collect sensitive children's data. Additionally, the OAG should be careful in drafting regulations to ensure that they do not open avenues for malicious actors to take advantage of new data troves and a need for new technology solutions to perpetuate scams or other harms. It will be important for the OAG's office to provide oversight and assistance to this sector to protect New Yorkers from any adverse impacts of age flags.

Further, if a user reaches the age of majority, there may be scenarios where a local site is able to detect such a user's newfound adult status. However, a universal signal based on potentially out-of-date biometric information, bank information, or cognitive test results would not pick this up. Any regulations must account for this complication or other scenarios where a user might use a VPN, chooses privacy settings that limit flags, multiple users on one device or browser, multiple browsers on one device, for example.

Finally, signals indicating a user's age or minor status based on a patchwork of third party data could be in conflict. "Government data, biometric information, bank information, or cognitive test results," in particular, could each create conflicting indicators as to whether or not a user is a minor.

**Question 3: Are there other factors or considerations related to obtaining informed consent that OAG regulations should consider?**

We would note that parents have been providing consent for their children under the age of 13 to use various online services for decades under COPPA. COPPA already establishes several acceptable methods of collecting parental consent. Over time, these methods have been updated to ensure maximum efficiency and to take into account technological trends.

Furthermore, many of the parental consent methods specified by COPPA apply just as well in the context of teens as they do to children under the age of 13. For example, requiring the use of a credit card in connection with a transaction is effective in filtering out teen users, as most such users would not have a credit card. Companies have developed methods to obtain consent in the ways specified by COPPA.

Additionally, the OAG should consider how companies may obtain parental consent without unduly burdening parents. Any method of parental consent should strive to minimize the number of times that a company is required to contact the parent to provide information or solicit additional consents. Instead, a single request for consent that outlines the information collected from the child and the various purposes for which a child's information may be used would allow the parent to be in control of their child's use of the service, while avoiding decision or information fatigue.

## Conclusion

Thank you for your time and consideration. If you have further questions, please contact Sara Kloek at skloek@siia.net or Anton van Seventer at avanseventer@siia.net.