September 26, 2024

Office of the New York State Attorney General, The Honorable Letitia James
New York State Capitol
State Street and Washington Avenue
Albany NY, 12224-0341
Submitted electronically at ChildDataProtection@ag.ny.gov

RE: Office of the New York Attorney General's Advanced Notice of Proposed Rulemaking pursuant to New York General Business Law section 899-ee *et seq*

Dear Attorney General James:

On behalf of the Computer & Communication Industry Association, I write in response to the Office of the New York State Attorney General's ("the Office's") Advanced Notice of Proposed Rulemaking pursuant to New York General Business Law section 899-ee *et seq*, the "Child Data Protection Act" ("CDPA").

CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] CCIA holds a firm conviction that children are entitled to a higher level of security and privacy in their online experiences. Our members are actively engaged in various initiatives to integrate robust protective design features into their websites and platforms.[2] CCIA's members have been leading the effort to implement settings and parental tools to individually tailor younger users' online use to the content and services that are suited to their unique lived experience and developmental needs. For example, various services allow parents to set time limits, provide enhanced privacy protections by default for known child users, and other tools to allow parents to block specific sites entirely.[3]

CCIA and its members commend the Office for its efforts to implement the requirements under the Child Data Protection Act swiftly and transparently. CCIA's enclosed responses are intended to reflect and focus on the Association's specific areas of expertise and do not represent an exhaustive response to each of the questions proposed by the Office.

We appreciate the opportunity to provide input as the rulemaking process is in its early stages and look forward to additional opportunities to engage with the Office.

1. "Primarily directed to minors"

Consistency with federal law and the U.S. Constitution

[1] For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.
[2] Jordan Rodell, *Why Implementing Education is a Logical Starting Point for Children's Safety Online*, Disruptive Competition Project (Feb. 7, 2023), https://www.project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/.
[3] Competitive Enterprise Institute, *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/.

CCIA recommends that any regulations strive to achieve consistency and interoperability with existing federal law, namely the Children's Online Privacy Protection Act (COPPA), as most online websites and services already have established systems to achieve compliance. Diverging from this long-standing set of established rules would not only risk bringing New York's law into conflict with COPPA, which would preempt New York's law, but would also create unnecessary confusion and friction for businesses covered under the CDPA.

Courts have ruled that laws can be unconstitutional if they make it burdensome for adults (and minors) to access speech that is protected by the U.S. Constitution[4]. To avoid making overly broad regulations that cover websites and services largely intended for adults, the Office should create clear and easy-to-follow rules based on objective, observable evidence. These rules should only apply to websites and services that are primarily for minors. Without clear rules for deciding which services are for teens and adults, the CDPA risks being too vague. A law is considered unconstitutional if it doesn't clearly convey what is prohibited or is so unclear that it allows for unfair enforcement. Without clear regulations on which services are covered, companies would not clearly understand compliance requirements and could face inconsistent enforcement.

Determining whether a website or service is "child-directed"

CCIA appreciates the Office's acknowledgment that the interests of older teens are likely to be "largely identical" to the interests of many adults. This point demonstrates why older teens should be treated differently than their younger peers in online spaces. Older teens may be employed, have hobbies or interests, or simply be researching topics that are more suited to and more common amongst older teens and adults. Therefore, older teens are likely to use and engage with online spaces in a similar way to those over the age of 18. The CDPA defines a child as anyone under 18. Due to the nuanced ways in which children under the age of 18 use the internet, it is imperative to appropriately tailor such treatments to respective age groups. For example, if a 16-year-old is conducting research for a school project, it is expected that they would come across, learn from, and discern from a wider array of materials than a 7-year-old on the internet playing video games. Any regulations would need to reflect the differences in how individuals under 18 use the internet in order to ensure that older teens are not treated the same as an early elementary school child.

As such, CCIA has previously suggested that older teens not be included in the scope of the legislation, but absent that change, the Office might consider establishing parameters surrounding whether users below a certain age (i.e., younger teens) are the target audience for a particular online service.

While it is important to assess whether websites or online services are primarily directed to minors or older teens, this also presents challenges. For example, it is more difficult to differentiate between similarly-aged peers, such as 17- and 18-year olds who may be classmates in high school. Both could have similar interests or conduct similar research for school projects, and therefore would likely have similar online footprints. It would be virtually impossible for a website provider to differentiate between the two without collecting

[4] United States v. Playboy Ent. Grp., Inc., 529 U.S. 803, 812 (2000) (holding that "The distinction between laws burdening and laws banning speech is but a matter of degree. The Government's content-based burdens must satisfy the same rigorous scrutiny as its content-based bans"); Ashcroft v. ACLU (Ashcroft II), 542 U.S. 656, 658-59 (2004).

significantly more sensitive data about every user, which would violate federal law and the CDPA.

Further, the lived experience of each individual user could significantly impact a variety of factors that impact how to assess whether websites or online services are primarily directed to minors or older teens. Humans in general, especially across younger and older teens, have very nuanced opinions surrounding what may be "age-appropriate" or "targeted" to them. The diverse lived experiences of children, teens, and adults vary significantly, leaving businesses without a comprehensive roadmap to navigate each user's unique perspective. Therefore, determining the optimal assessment criteria for whether a website or online service is "primarily directed" to certain specific age groups, let alone any specific individual engaging with an online platform, poses a serious feasibility challenge.

The Office could use the COPPA Rule's factors for determining if a service is child-directed, but may consider focusing more on factors like audience demographics, advertisements and marketing, and the complexity of language used by the service. These factors are more likely to help distinguish between services that appeal to teens and those that appeal to adults. Factors like subject matter, visual and audio design, and the age of models might be less important because they are less likely to be different for teen and adult-directed services. The Office might also consider whether a website primarily contains content that would generally be considered to be attractive and targeted to a child. For example, certain websites might include characters that are popular among children or language that is geared toward users of a particular reading level.

Shifts in audience outside of the website's or service's control

CCIA recommends that the Office treat websites and online services differently, taking into consideration that there are many factors outside their control whereby users generally, and especially minors, may become attracted to new types of content. Without doing so, it is conceivable that every website or online service would be required to conform to standards intended to serve the youngest internet users, fearing that if their platform becomes popular with users based on a shift in public sentiment or a trend, they could be liable for potential violations.

This would place website and online services in an untenable position of needing to constantly shift to immediately comply with this law, because their audience could once again shift back towards those over 18. If a website's audience has solidly shifted to younger internet users, the Office might consider establishing time frames associated with an audience shift (i.e., if the predominant known audience age over the course of a 12-month period is below a certain age threshold) then the website operator or online service should have to comply with the law. This would help provide enough time to determine whether the shift is temporary or long-term and simultaneously allow the service adequate time to comply.

Portions of websites or online services

The task of differentiating between various "portions" of a website is extremely difficult and therefore, we suggest that the Office not distinguish between "portions" of a website unless those portions are a separate experience in which internet operators could feasibly undertake separate compliance processes for that portion of the site as opposed to the rest of the

platform. Instances such as a video streaming channel hosted on a platform that serves family-friendly content, should not be treated as a separate portion of the service because to do so would degrade the experience on such platforms for consumers, who would be constantly forced to navigate through consent requests.

2. "Personal data"

The regulations should specifically lay out that any anonymized or deidentified data that is not re-linked to a specific individual should be treated differently, as this would still allow websites and online services to use such data for product development or consumer feedback that could be used to improve the user experience. This would also put New York in line with other existing state consumer privacy laws.

3. "Permissible processing"

Factors to consider in defining what processing is "strictly necessary" to be permissible without requiring specific consent

In defining what processing is "strictly necessary" to be permissible under the CDPA without requiring specific consent, the Office should consider several factors. These include functions inherent to the service, reasonable user expectations, and first-party processing. Considering each of these factors will ensure that the totality of a covered entity's functionality is permissible. This will enable consumers to continue the personalized experience that they have grown accustomed to, such as receiving recommendations for the next video in a series of instructional videos about algebra after viewing the first in the series.

CCIA encourages the Office to avoid adopting an unnecessarily narrow interpretation of "strictly necessary" that might otherwise limit safer online experience for younger users. For example, services may process personal data to improve and develop products that offer safer experiences for younger users such as flagging inappropriate content or language in message boards, social posts, or chats. Processing for such expected purposes should not require additional informed consent, as this would only serve to inundate younger users with consent requests, which is likely to result in consent fatigue and create a disruptive experience that is inconsistent with user expectations.

Permissible processing pursuant to internal business operations

Consistent with CCIA's earlier comments regarding maintaining consistency and interoperability with existing federal law, CCIA recommends that any new regulations adhere to current rules established under COPPA regarding permitted processing for "internal business operations." These include: (i) maintaining or analyzing the functioning of the website or online service; (ii) performing networking communications; (iii) authenticating users and personalizing the content on the website or online service; (iv) serving contextual advertising on the website or online service or cap the frequency of advertising; (v) protecting the security or integrity of the user, website, or online service; (vi) ensuring legal or regulatory compliance, or; (vii) fulfilling a specific request from a minor.

4. "Informed consent"

Soliciting informed consent from teen users

The Office proposes several questions regarding how covered companies can solicit informed consent from teen users. It is important that requests for consent from teen users balance effectively conveying information to users without overwhelming users with excessive information or requests.

CCIA also recommends that any promulgated rules recognize the inherent differences between teen users and younger users. Teens tend to have a more sophisticated understanding of language than child audiences and more experience navigating online spaces. Therefore, the Office might consider mirroring requirements for notices that have been adopted more broadly under data privacy frameworks, ensuring that all language included in any notice be written in plain language, as to avoid any confusing technical terms. For example, the Colorado Department of Law issued regulations specifying that disclosures to consumers must be "understandable and accessible to a Controller's target audiences, considering the vulnerabilities or unique characteristics of the audience and paying particular attention to the vulnerabilities of Children. For example, they shall use plain, straightforward language and avoid technical or legal jargon."[5]

Consent mechanisms can be a powerful tool for promoting transparency and consumer control. However, it is important to recognize that the provision of many services, both online and offline, requires the collection and processing of certain user information. CCIA suggests that the Office avoid overly prescriptive rules that would require covered businesses to serve an unwieldy number of consent notices to users as this may contribute to "consent fatigue" while simultaneously degrading the user experience and overwhelming the user.[6] To that end, the Office might consider rules that clarify that a covered business can communicate multiple relevant ideas in one notice provided to the user.

5. "Parental consent"

Parental consent methods consistent with federal law

Websites and online services employ a variety of methods to determine whether an individual is the parent or guardian of a given user consistent with compliance requirements established under COPPA. These methods might include uploading a government-issued photo identification card, using a credit, debit, or other online payment method, or verification via video conferencing to confirm identity. CCIA encourages the Office to craft regulations that align with the methods that are currently used in the parental verification process for compliance with COPPA. The costs associated with different verification methods vary depending on the type of service and the necessary mechanisms required to successfully implement them. However, given that many businesses already have mechanisms in place to comply under COPPA, this would present the most frictionless framework for businesses to comply with under the CDPA.

[5] *See* Colorado Privacy Act Rules, 4 CCR-904-3, Rule 3.02, https://coag.gov/app/uploads/2022/10/CPA_Final-Draft-Rules-9.29.22.pdf.

[6] See Article 29 Data Protection Working Party, WP 259, *Guidelines on Consent Under Regulation 2016/679*, 17 (Apr. 10, 2018), ("In the digital context, many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day. This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing."), https://ec.europa.eu/newsroom/article29/items/623051.

Other factors or considerations related to obtaining parental consent

CCIA encourages the Office to consider how covered businesses under the CDPA would operationalize parental consent requirements and associated equity concerns. There are significant challenges associated with verifying whether a "parent or guardian" is a specific minor's legal parent or guardian. Many parents and legal guardians do not share the same last name as their children due to remarriage, adoption, or other cultural or family-oriented decisions. If there is no authentication that a "parent or guardian" is that specific minor's legal parent or guardian, this may incentivize minors to ask other adults who are not their legal parent or guardian for consent. It is also unclear who would be able to give consent to a minor in foster care or other nuanced familial situations, creating significant equity concerns. Further, scenarios where a legal parent or guardian is not located in New York or is not a resident of the state create significant confusion for consumers and businesses.

Further, some portion of the population may not have access to one or several of the means necessary to establish such verification, such as lack of government identification or any form of banking. Furthermore, there are populations that have knowledge limitations when it comes to navigating online spaces and therefore could be incapable of navigating through any such verification process. Any such requirements should avoid unduly burdening parents, as parents too can become susceptible to consent fatigue, which may end up hindering younger individuals' ability to access the internet.

* * * * *

We appreciate the consideration of these comments and stand ready to provide additional information regarding technology policy. Should you have any questions, please do not hesitate to reach out to me at aspyropoulos@ccianet.org.

Sincerely,

Alexander Spyropoulos
Regional Policy Manager, Northeast
Computer & Communications Industry Association