



June 5, 2024

House Committee on Children & Youth  
Capitol Building  
501 North Third Street  
Harrisburg, PA 17120

**Re: HB 1879 - "An Act providing for duties of covered entities to protect the best interests of children that use online services, products or features and for data protection impact assessments; prohibiting certain actions by covered entities; and imposing penalties." (Oppose)**

Dear Chair Bullock and Members of the House Committee on Children & Youth:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 1879 in advance of the House Committee on Children & Youth hearing on June 5, 2024.

CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.<sup>1</sup> Proposed regulations on the interstate provision of digital services therefore can have a significant impact on CCIA members. Acknowledging policymakers' valid concerns about the online privacy of young individuals, it is imperative to prioritize the establishment of a comprehensive data privacy law applicable to all consumers. This law should incorporate safeguards for sensitive data, specifically addressing information commonly linked to younger users.

CCIA holds a firm conviction that children are entitled to a higher level of security and privacy in their online experiences. Presently, our members are actively engaged in various initiatives to integrate robust protective design features into their websites and platforms.<sup>2</sup> 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.<sup>3</sup> This is also why CCIA supports the implementation of digital citizenship curriculum in schools, to not only educate children on proper social media use but also help educate parents on how they can utilize existing mechanisms and tools to protect their children the way they see fit.<sup>4</sup>

It should also be recognized that protecting children from harm online does not include a generalized power to restrict ideas to which one may be exposed. Speech that is neither

---

<sup>1</sup> 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>.

<sup>2</sup> 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/>.

<sup>3</sup> Competitive Enterprise Institute, *Children Online Safety Tools*, <https://cei.org/children-online-safety-tools/>.

<sup>4</sup> See *supra* note 2.

obscene to young people nor subject to other legitimate laws cannot be suppressed solely to protect young online users from ideas or images that a legislative body disfavors. Proposals to keep children safe online should be established through a risk-based approach to developing protections for different ages of users and by focusing on tangible harm. While CCIA shares the goal of increasing online safety, HB 1879 presents the following concerns.

### **The bill lacks narrowly tailored definitions.**

As currently written, the bill 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. We suggest changing the definition of “child” to a user under the age of 13 to align with the federal Children’s Online Privacy Protection Act (COPPA) standard. This would also allow for those over 13, who use the internet much differently than their younger peers, to continue to benefit from its resources. The definition of “likely to be accessed by children” is also ambiguous. CCIA recommends narrowly tailoring this definition to content intentionally targeted at or branded for children when they are using the internet.

The definition of “best interests of a child” is incredibly vague and impossible to operationalize at scale, creating moving goalposts for compliance. The benefit of a dynamic marketplace is that online businesses are able to tailor their services and products to what is most relevant and useful to their specific audience. Private online businesses will not be able to coherently or consistently make diagnostic assessments of users, including their mental and physical health. Humans in general, especially children, have very nuanced opinions surrounding what may be harmful 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. Determining the optimal solutions for the well-being of each and every young individual engaging with an online platform poses a serious feasibility challenge.

### **The bill does not provide how a user’s age will be estimated and how penalties for those who do not abide by the law will be enforced.**

In order to achieve meaningful children’s safety protections, it is imperative for businesses to have a roadmap of how to properly comply and avoid unintentional violations.<sup>5</sup> This measure provides broad strokes of *what* is expected of businesses but does not portend *how* businesses may achieve those objectives. Instead, businesses may be allowed to “profile a child by default” under certain circumstances. CCIA interprets this as necessitating businesses to distinguish users aged below and above 18. We recommend providing clarity on the procedures businesses should follow to determine the age of users online, specifically when “profiling” them as children. Without a proper mechanism in place, businesses may encounter challenges in accurately determining the age of each individual user, potentially resulting in unintended violations for which the business may be held liable.

---

<sup>5</sup> Digital Trust & Safety Partnership, *Age Assurance: Guiding Principles and Best Practices* (Sept. 2023), [https://dtspartnership.org/wp-content/uploads/2023/09/DTSP\\_Age-Assurance-Best-Practices.pdf](https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf).

CCIA cautions against conflating concepts regarding estimating the age of users.<sup>6</sup> For example, when a website asks a user to make a self-attestation of their age, such as on a website for alcohol products, the owner of that website is not held liable if that user chooses to mischaracterize their identity. Similar self-attestation measures are currently in place for social media platforms and other digital services, and the burden is on the consumer to be forthcoming and honest about the age and birthdate they enter. This, however, would change under HB 1879 — if online services were to rely on self-attestation for estimates but then in-turn be held liable for mischaracterizations, this would unreasonably treat the business as the bad actor. Further, it is unclear what impact the use of VPNs and similar mechanisms to evade state-specific age verification requirements by users could have on organizations' liability under this bill.

To achieve compliance and avoid the proposed penalties for violations, it is likely that age estimation would effectively amount to age verification. Current commercially available facial recognition and other mechanisms that provide age estimation cannot sufficiently accomplish what lawmakers are expecting.<sup>7</sup> The AADC purports not to require age verification, but the definitions and policy itself are so vague that sites will have no choice but to implement some kind of age verification technology to achieve compliance. Such verification requirements then raise questions about potential conflicts with data minimization principles and other consumer data privacy protection measures.

CCIA is concerned that businesses may be forced to collect age verification data, which would paradoxically force companies to collect a higher volume of data on children.<sup>8</sup> Businesses may be forced to collect personal information they don't want to collect and consumers don't want to give, and that data collection creates extra privacy and security risks for everyone. Further, the Commission Nationale de l'Informatique et des Libertés (CNIL) analyzed several existing online age verification solutions but found that none of these options could satisfactorily meet three key standards: 1) providing sufficiently reliable verification; 2) allowing for complete coverage of the population; and 3) respecting the protection of individuals' data, privacy, and security.<sup>9</sup> Though the intention to keep kids safe online is commendable, this bill is counterproductive to that initiative by requiring more data collection about young people.

---

<sup>6</sup> Khara Boender, *Children and Social Media: Differences and Dynamics Surrounding Age Attestation, Estimation, and Verification*, Disruptive Competition Project (May 10, 2023), <https://www.project-disco.org/privacy/children-and-social-media-differences-and-dynamics-surrounding-age-attestation-estimation-and-verification>.

<sup>7</sup> Berin Szóka, *Comments of TechFreedom In the Matter of Children's Online Privacy Protection Rule Proposed Parental Consent Method; Application of the ESRB Group for Approval of Parental Consent Method*, TechFreedom (Aug. 21, 2023), <https://techfreedom.org/wp-content/uploads/2023/08/Childrens-Online-Privacy-Protection-Rule-Proposed-Parental-Consent-Method.pdf>.

<sup>8</sup> Caitlin Dewey, *California's New Child Privacy Law Could Become National Standard*, The Pew Charitable Trusts (Nov. 7, 2022), <https://pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/11/07/californias-new-child-privacy-law-could-become-national-standard>.

<sup>9</sup> *Online age verification: balancing privacy and the protection of minors*, CNIL (Sept. 22, 2022), <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>.



**Over the past two years, changes to the Age-Appropriate Design Code have been proposed, including those in HB 1879, aimed at addressing constitutional concerns found in the original version. However, these new changes fail to resolve those issues.**

In 2022, California enacted its version of the Age-Appropriate Design Code. However, the law is currently on hold due to a legal challenge over constitutional issues created by its broad and vague requirements. Moreover, the law, similar to Pennsylvania’s HB 1879, contains data protection impact assessment requirements for online businesses. These are considered compelled commercial disclosures because a law that allows the government to search and seize sensitive business information is “facially invalid” if it doesn’t give the business a chance to contest the order to turn over the records. For all of these reasons, the court held that the law regulates protected expression and that, regardless of whether the Act is subject to strict scrutiny or intermediate scrutiny, the law likely violates the First Amendment. Given that HB 1879 contains similar vague and overburdensome requirements, it is probable that the bill could also raise constitutional concerns.

\* \* \* \* \*

While we share the concerns of the sponsor and the House Committee on Children & Youth regarding the safety of young people online, we encourage Committee members to resist advancing legislation that is not adequately tailored to this objective. We appreciate the Committee’s consideration of these comments and stand ready to provide additional information as the Legislature considers proposals related to technology policy.

Sincerely,

Jordan Rodell  
State Policy Manager  
Computer & Communications Industry Association