April 10, 2024

The Office of the Honorable Wes Moore, Governor of Maryland
State Capitol
100 State Circle
Annapolis, MD 21401

RE: SB 571/HB 603 - "Consumer Protection – Online Products and Services – Data of Children (Maryland Kids Code)" (Veto Request)

Dear Governor Moore:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully request a veto on SB 571/HB 603.

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. Presently, 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]

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 what mechanisms presently exist that they can use now to protect their children the way they see fit and based on their family's lived experiences.[4] In fact, in 2023, the Maryland Senate introduced SB 799 which aimed at enhancing media literacy skills in young people, including through the requirement to develop and publish a cyber safety guide that, among other things, would be used to promote good decision-making when using online media and responsible internet use. Unfortunately, that legislation did not pass the General Assembly and the effort was not re-introduced this session.

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 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

[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/.
[4] *See supra* note 2.

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, this bill presents the following concerns.

The bill lacks narrowly tailored definitions necessary to achieve compliance.

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 bill would also require businesses to provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using "clear language suited to the age of children likely to access that online service, product, or feature". The definition of "clear language suited to the age of children likely to access the online product" is not defined and leaves room for significant subjective interpretation. If a child is defined as anyone under 18, one could expect a wide variation of reading comprehension skills across such a wide age group — a 17-year-old would presumably have better reading comprehension skills than that of a 5-year-old. Without "clear language" being defined, the bill would be difficult to comply with.

Additionally, the definition of "best interests of children" is incredibly vague and impossible to operationalize at scale, creating moving goalposts for compliance. The benefit of a dynamic marketplace is that online businesses can 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 what could be "physically, financially, or emotionally" harmful to them. 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's provisions addressing the "profiling" of a child and the enforcement of penalties for violations pose significant questions regarding compliance.

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.[5] 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.

CCIA cautions against conflating concepts regarding "profiling" or estimating the age of users.[6] 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 birth date they enter. This, however, would change under SB 571/HB 603 — 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 "profiling" or 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.[7] The Maryland Kids Code 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, and unfortunately, SB 571/HB 603's approach includes these same pitfalls. Such verification requirements then raise questions about potential conflicts with data minimization principles and other consumer data privacy protection measures.

---

[5] 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.

[6] 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.

[7] 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.

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.[8] 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.[9] 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.

Restricting access to the internet for younger users curtails their First Amendment right to information, denying them entry to supportive online communities that might be unavailable in their local physical location.

The First Amendment, including the right to access information, is applicable to teens. Vague restrictions on protected speech cannot be justified in the name of "protecting" minor users online nor is a state legislative body the arbiter of what information is suitable for younger users to access. Moreover, when businesses are required to deny access to social networking sites or other online resources, this may also unintentionally restrict children's ability to access and connect with like-minded individuals and communities. For example, children of racial or other minority groups may not live in an area where they can easily connect with others that represent and relate to their own unique experiences. An online central meeting place where kids can share their experiences and find support can have positive impacts.

The hyperconnected nature of social media has led many to allege that online services may be negatively impacting teenagers' mental health. However, some researchers argue that this theory is not well supported by existing evidence and repeats a "moral panic" argument frequently associated with new technologies and new modes of communication. Instead, social media effects are nuanced,[10] small at best, reciprocal over time, and gender-specific. Additionally, a study conducted by researchers from Columbia University, the University of Rochester, the University of Oxford, and the University of Cambridge found that there is no evidence that associations between adolescents' digital technology engagement and mental health problems have increased.[11] Particularly, the study shows that depression's relation to both TV and social media was practically zero. The researchers also acknowledged that it is possible, for example, that as a given technology becomes adopted by most individuals in a group, even individuals who do not use that technology could become indirectly affected by it,

[8] 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.
[9] *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.
[10] Amy Orben *et al.*, *Social Media's enduring effect on adolescent life satisfaction*, PNAS (May 6, 2019), https://www.pnas.org/doi/10.1073/pnas.1902058116.
[11] Amy Orben, Andrew K. Przybylski, Matti Vuorre, *There Is No Evidence That Associations Between Adolescents' Digital Technology Engagement and Mental Health Problems Have Increased*, Sage Journals (May 3, 2021), https://journals.sagepub.com/doi/10.1177/2167702621994549.

either through its impacts on peers or by them being deprived of a novel communication platform in which social life now takes place.

Related proposals with similar requirements for online businesses are currently being litigated in several different jurisdictions.

When the federal Communications Decency Act was passed, there was an effort to sort the online population into children and adults for different regulatory treatment. That requirement was struck down by the U.S. Supreme Court as unconstitutional because of the infeasibility.[12] After 25 years, age authentication still remains a vexing technical and social challenge.[13] California, Arkansas, and Ohio recently enacted legislation that would implement age verification and estimation requirements — each law is currently facing a legal challenge due to constitutional concerns, and judges recently put both laws on hold until these challenges can be fully reviewed.[14] The fate of a similar law in Utah is also in jeopardy as it is also facing legal challenges.[15] **CCIA believes that requiring covered websites to treat users under and over 18 years of age differently would mandate the use of age verification mechanisms. Even with the amendments made by both the House and Senate for HB 603/SB 571, these requirements are likely to raise similar constitutional concerns and significantly fail to meet constitutional standards.** We have raised these concerns with the bill sponsors, the members of the House Economic Matters Committee, and the members of the Senate Finance Committee. CCIA recommends that lawmakers permit this issue to be more fully examined by the judiciary before burdening businesses with legislation that risks being invalidated and *passing on expensive litigation costs to taxpayers.*

* * * * *

While we share your concerns regarding the safety of young people online, we encourage you to resist signing legislation that is not adequately tailored to this objective, and we respectfully request a veto of SB 571/HB 603.

We appreciate your consideration of these comments and stand ready to provide additional information related to technology policy.

Sincerely,

Jordan Rodell
State Policy Manager
Computer & Communications Industry Association

[12] *Reno v. ACLU*, 521 U.S. 844 (1997).
[13] Jackie Snow, *Why age verification is so difficult for websites*, The Wall Street Journal (Feb. 27, 2022), https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728.
[14] *NetChoice, LLC v. Bonta* (N.D. Cal. 5:22-cv-08861); *NetChoice, LLC v. Griffin* (W.D. Ark. 5:23-cv-05105; *NetChoice, LLC v. Yost* (S.D. Ohio 2:24-cv-00047)).
[15] *NetChoice, LLC v. Reyes* (D. Utah 2:23-cv-00911); *Zoulek et al. v. Hass & Reyes* (D. Utah 2:24-cv-00031).