June 13, 2023

The Ohio State House
1 Capitol Square
Columbus, Ohio 43215-4275

RE: HB 33 - "Establishes operating appropriations for fiscal years 2024-2025" (Oppose Unless Amended)

Dear Representative:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 33 unless it is amended to **remove Sec. 1349.09.**

CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] Proposed regulations on the interstate provision of digital services therefore can have a significant impact on CCIA members. Recent sessions have seen an increasing volume of state legislation related to the regulation of digital services. While recognizing that policymakers are appropriately interested in the digital services that make a growing contribution to the U.S. economy, these bills require study, as they may raise constitutional concerns, conflict with federal law, and risk impeding digital services companies in their efforts to restrict inappropriate or dangerous content on their platforms.[2]

CCIA strongly believes children deserve an enhanced level of security and privacy online. Currently, there are a number of efforts among our members to incorporate protective design features into their websites and platforms.[3] CCIA's members have been leading the effort in raising the standards for teen safety and privacy across our industry by creating new features, settings, parental tools, and protections that are age-appropriate and tailored to the differing developmental needs of young people.

While CCIA strongly supports the overall goal of keeping children safe online, there are many concerns we would like to raise about the policies Sec. 1349.09 of HB 33 would implement.

1. Sec. 1349.09 of HB 33 regarding liability for age verification and parental approval will not achieve its stated objectives. In fact, the provision may actually put Ohioans at greater risk of harm, including children that the legislation seeks to protect.

This legislation will inevitably result in companies being required to collect additional information about all users, including adults. Sec. 1349.09 does not provide how businesses are to obtain the age of users. CCIA suggests clarifying how businesses are expected to know the age of users online. Without a proper mechanism in place, it is difficult for businesses to discern the age of every individual user which could lead to unintended violations. To achieve compliance and avoid the proposed penalties for violations, it is likely that these requirements would amount to age verification which raises questions about whether such verification

[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] Taylor Barkley, Aubrey Kirchhoff, & Will Rinehart, *5 things parents and lawmakers need to know about regulating and banning social media*, The CGO (Mar. 7, 2023), https://www.thecgo.org/benchmark/5-things-parents-and-lawmakers-need-to-know-about-regulating-and-banning-social-media/.
[3] 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/.

mechanisms would conflict with data minimization principles and other consumer data privacy protection measures. CCIA is concerned that businesses may be forced to collect geolocation and age verification data, which would paradoxically force companies to collect a higher volume of data on users.[4] Businesses may be forced to accumulate personal information they do not want to collect and consumers do not want to give, and that data collection creates extra privacy and security risks for everyone. This mandated data collection would include collecting highly sensitive personal information about children and their parents, including collecting and storing their geolocation to ensure they do not reside outside of the state when confirming that they are of age to be using these services. If the state were to force companies to collect a higher volume of data on users even as others are requiring the collection of less data, it may place businesses in an untenable position of picking which state's law to comply with, and which to violate.

Further, Sec. 1349.09 of HB 33 would hold covered social media companies liable for failing to receive parental consent but also prohibits a social media company from retaining identifying information about the parent after access is granted. However, by requiring covered businesses to delete relevant information, the law would leave businesses without a means to document their compliance. This becomes especially problematic in instances where a user decides to use deceptive verification information such as using an identification card that is not their own. Additionally, it is unclear what impact users' employment of VPNs and other mechanisms to evade age verification and parental approval could have on organizations' liability under this provision.

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.[5] After 25 years, age authentication still remains a vexing technical and social challenge.[6] California recently enacted legislation that would implement similar age verification measures which is currently being challenged for similar reasons.[7] CCIA recommends that lawmakers permit this issue to be more fully examined by the judiciary before burdening businesses with legislation that risks being invalidated.

2. Sec. 1349.09 of HB 33 may result in shutting down services for all users under 16, including access to supportive communities that may not be available in their physical location.

The Children's Online Privacy Protection Act (COPPA) and associated rules at the federal level currently regulate how to address users under 13, a bright line that was a result of a lengthy negotiation process that accounted for the rights of users and children while also considering the compliance burden on businesses. To avoid collecting data from users under 13, some businesses chose to shut down various services when COPPA went into effect due to regulatory complexity – it became easier to simply not serve this population. Users between 14 and 15 could face a similar fate as HB 33 would implement more complex vetting requirements tied to parental consent for users under 16.

[4] Caitlin Dewey, *California's New Child Privacy Law Could Become National Standard*, The Pew Charitable Trusts (Nov. 7, 2022), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/11/07/californias-new-child-privacy-law-could-become-national-standard.
[5] *Reno v. ACLU*, 521 U.S. 844 (1997).
[6] 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.
[7] *NetChoice v. Bonta* (N.D. Cal. 22-cv-08861).

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, in instances where children may be in abusive or unsafe households, this could create an impediment for children seeking communities of support or resources to get help.

Serious concerns also arise when verifying whether a "parent or guardian" is, in fact, a child'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 actually a child's legal parent or guardian, this may incentivize children to ask other adults that are not their legal parent or guardian to verify their age on behalf of the child to register for an account with an "operator." It is also unclear who would be able to give consent to a child in foster care or other nuanced familial situations, creating significant equity concerns. Further, scenarios where a legal parent or guardian is not located in Ohio or is not a resident of the state creates significant confusion for consumers and businesses.

An online central meeting place where younger users can share their experiences and find support can have positive impacts. Teens themselves paint a nuanced picture of the effects of social media. It is one in which majorities credit these platforms[8] with deepening connections and providing a support network when they need it. In a recent survey, 80% of teens say that what they see on social media makes them feel more connected to what's going on in their friends' lives, while 71% say it makes them feel like they have a place where they can show their creative side. Additionally, 67% also say these platforms make them feel as if they have people who can support them through tough times.

3. Sec. 1349.09 of HB 33 lacks narrowly tailored definitions and thresholds.

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. This measure provides broad strokes of *what* is expected of businesses but does not portend *how* businesses may achieve those objectives. For example, as currently written, Sec. 1349.09 does not define "reasonably anticipated to be accessed by children." CCIA recommends narrowly tailoring this definition to content intentionally targeted at or branded for children when they are using the internet. Otherwise, this leaves room for significant subjective interpretation. It is reasonable to anticipate that children could access any website or app when using the internet, even if they are not intentionally targeted or branded for children. For example, AARP has resource guides for caregivers and their families.[9] Though children are not their target audience for these resources, children may seek out this information when looking for support on how to cope with a grandparent that has been diagnosed with dementia.

Additionally, though "operators" are required to receive parental consent if their services are "reasonably anticipated to be accessed by children," and a list of factors (loosely mirroring the factors in COPPA) is included, the provision does not include a threshold requirement or a mixed audience exception. This is important to include because, for example, if the attorney general or court found that two of the several factors of a site or app could be "reasonably anticipated to be accessed by children," it is difficult to know if that would be sufficient for a violation. Without clear definitions and thresholds, especially with the overly

[8] Monica Anderson *et al.*, *Connection, creativity and drama: Teen life on social media in 2022*, Pew Research Center: Internet, Science & Tech (Nov. 17, 2022), https://www.pewresearch.org/internet/2022/11/16/connection-creativity-and-drama-teen-life-on-social-media-in-2022/.
[9] AARP, *AARP resources for caregivers and their families*, AARP Family Caregiving (June 8, 2023) https://www.aarp.org/caregiving/.

broad definition of an "operator", the law is difficult to comply with, and difficult for businesses to avoid liability.

4. Businesses operating online depend on clear regulatory certainty across jurisdictions nationwide.

Existing U.S. law provides websites and online businesses with legal and regulatory certainty that they will not be held liable for third-party content and conduct. By limiting the liability of digital services for misconduct by third-party users, U.S. law has created a robust internet ecosystem where commerce, innovation, and free expression thrive — all while enabling providers to take creative and aggressive steps to fight online abuse. Ambiguous and inconsistent regulation at the state level would undermine this business certainty and deter new entrants, harming competition and consumers. This particularly applies to new small businesses that tend to operate with more limited resources and could be constrained by costs associated with compliance. While larger companies may be able to more easily absorb such costs, it could disproportionately prevent new smaller start-ups from entering the market.

Further, careful consideration of what constitutes best practice should involve conversations with practitioners and relevant stakeholders. Online businesses are already taking steps to ensure a safer and more trustworthy internet — recently, leading online businesses announced[10] that they have been voluntarily participating in the Digital Trust & Safety Partnership (DTSP) to develop and implement best practices and recently reported on the efforts to implement these commitments.[11] We urge lawmakers to study both the benefits and drawbacks of teen safety and privacy requirements and to engage with practitioners and stakeholders to support the ongoing development of practicable solutions.

* * * * *

While we share the concerns raised regarding the safety of young people online, we encourage legislators to resist advancing **Sec. 1349.09 of HB 33** which is not adequately tailored to this objective. We believe it was a pragmatic choice for the House to omit this proposal in their version of the budget, and we encourage the Senate to follow their lead.

We appreciate your 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

[10] Margaret Harding McGill, *Tech giants list principles for handling harmful content*, Axios (Feb. 18, 2021), https://www.axios.com/techgiants-list-principles-for-handling-harmful-content-5c9cfba9-05bc-49ad-846a-baf01abf5976.html.
[11] *See, e.g.*, DTSP, *The Safe Assessments: An Inaugural Evaluation of Trust & Safety Best Practices* (July 2022), https://dtspartnership.org/wp-content/uploads/2022/07/DTSP_Report_Safe_Assessments.pdf (Appendix III: Links to Publicly Available Company Resources), at 37.