January 25, 2024

Senate Commerce and Technology Committee
200 W. Washington Street
Indianapolis, IN 46204

RE: SB 201 - "Minor use of mobile devices and social media." (Oppose)

Dear Chair Buchanan and Members of the Senate Commerce and Technology Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SB 201.

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. In recent sessions, there has been a notable surge in state legislation concerning children's online safety. CCIA and our member companies have a shared interest in ensuring strong protections are in place to protect children and provide parents and adults with simple but effective tools to provide a safe online environment for their families.

CCIA holds a firm conviction that children are entitled to a higher level of security and privacy in their online experiences. Our members continue to invest heavily to provide robust protective features in their devices, websites, services, and platforms.[2] CCIA's members are leading global efforts to implement settings and parental tools to individually tailor younger users' online use to the content and services that are suited to age, unique lived experiences, and developmental needs. For example, best practices currently in place 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]

In addition to strong technology features, CCIA supports the implementation of digital citizenship curriculum in schools to educate children, parents, teachers, and administrators about online safety and social media use to learn about technology features and existing mechanisms they can use now to protect their children.[4] We laud the efforts of both the Indiana Senate and the House on their introduction of SB 287 and HB 1253 this session requiring instruction regarding internet safety and media literacy in school curriculum.

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 thinks are unsuitable for them. 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.

---

[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.

While CCIA strongly supports the overall goal of keeping children safe online, requiring a state-specific default filter is technologically infeasible and would create unobtainable expectations with regard to content that filters can reasonably block. Typically, internet service providers (ISPs) govern which websites users can access. For example, known pirating sites are blocked by ISPs, not the manufacturer who produces the devices. It is also important to note that mobile devices do not have the capability of enabling a filter and other protective features within the borders of a single state, much less change as a mobile device is transported from one state to another.

We appreciate the opportunity to further expand on our concerns with the proposed legislation.

1. There is a robust market with widely available options across a variety of platforms, operating systems, and devices for consumers and parents to manage and restrict access to certain content.

Currently, there are many different filter technologies in a robust and competitive marketplace that provides users with a wide range of choices, quality, and cost. Mandating that a device activate an "adult content filter" undermines competition for competing products and ignores the different approaches to providing effective protection for networks, devices, and individual applications. Further, there is no "one size fits all" filter that addresses all potential concerns, including adult websites, scenes in mainstream movies, explicit lyrics in recorded music or videos, and a wide variety of adult-themed content that can be found online in a variety of formats. Different technology filters exist to address different types of content for different media, including videos, music, audio recordings, websites, written materials, and visual images. It is important to note, however, that while there are many different types of protection technologies to address a wide range of potential harms, no filter is infallible. A law that sets unrealistic expectations for protection that are technologically impossible is a law that will fail to meet its intended purpose, resulting in consumer frustration and costly litigation.

By requiring a content filter intended to prevent younger users from accessing certain content ignores the fact that adults, by and large, are the primary users of the cellular phone and tablet devices that the bill explicitly seeks to regulate. In the global economy, there are many products and services that we use that are not, by default, designed for younger users. For example, automobiles are designed with seats and seatbelts for adult consumers. However, car seats designed specifically for children's safety are available and recommended for use to ensure that children are as safe as possible when riding in an automobile. In a similar vein, many devices and services have content filtering technologies that allow parents to individually tailor settings and preferences to enable both adults and children to make appropriate choices about the type of content and services they can see and use[5]. These types of filters and settings, however, are not activated by default. SB 201 could invite significant consumer confusion for adults who are not aware such filters aimed for children are set by default. CCIA would recommend that the use of such filters continue to be voluntary and an opt-in feature for the specific consumers who wish to utilize them.

[5] Peggy Grande, G*overnment legislation for online content-filtering could roll back parental rights*, The Washington Times (Nov. 27, 2023), https://www.washingtontimes.com/news/2023/nov/27/government-legislation-for-online-content-filterin/\.

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

Ambiguous and inconsistent regulation at the state or local levels would undermine business certainty, creating significant confusion surrounding compliance. This type of regulatory patchwork may deter new entrants, harming competition, innovation, and consumers. Devices sold into a national market are not and cannot be designed for functionality to trigger by the mere fact that they have moved within a state's borders.

Further, SB 201 creates significant liability concerns due to the subjective nature of what may be considered "obscene matter" or "harmful". Individual or community perceptions often vary considerably, which creates potential legal liability for companies that fail to meet dynamic and subjective norms as a device is moved from one place to another – this is technologically implausible.

3. SB 201's provisions regarding liability for data collection and age verification will not achieve the bill's stated objectives.

SB 201 would hold covered social media companies liable for failing to perform age verification. The bill's obligation to collect additional information associated with age verification is itself likely to conflict with data minimization principles inherent in typical federal and international privacy and data protection compliance practices. 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 unintentionally violate.[6] A recent study from the Pew Research Center found that many Americans worry about children's online privacy but when asked about who is responsible for protecting children's online privacy, most (85%) say parents hold a great deal of responsibility for protecting kids' online privacy. 59% also say that tech companies bear the responsibility while 46% believe the government does. The study also highlights why it is important to consider the tradeoffs associated with age verification and consent proposals that would require the additional collection data; around 89% of Americans are very or somewhat concerned about social media platforms knowing personal information about kids.[7]

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.[8] Additionally, it is unclear what impact users' employment of virtual private networks (VPNs)[9] and other mechanisms to avoid location-specification age verification requirements could have on organizations' liability under this bill. 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.

---

[6] 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.

[7] Colleen McClain, *How americans view data privacy*, Pew Research Center: Internet, Science & Tech (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.

[8] *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.

[9] Cristiano Lima, *Utah's porn crackdown has a VPN problem*, The Washington Post (May 5, 2023), https://www.washingtonpost.com/politics/2023/05/05/utahs-porn-crackdown-has-vpn-problem/.

4. This legislation may halt services for individuals under 18, hindering teenagers' internet access and, consequently, restricting their First Amendment right to information. This includes access to supportive online communities that might 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 all users, including 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 17 could face a similar fate as SB 201 would implement more complex vetting requirements tied to parental consent for users under 18.

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 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 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 actually a minor's legal parent or guardian, this may incentivize minors to ask other adults who are not their legal parent or guardian to verify their age on behalf of the minor to register for an account with a "large social media platform." 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 Indiana or is not a resident of the state creates significant confusion for consumers and businesses.

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

[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.

5. Age verification and parental consent requirements for online businesses are currently being litigated in several 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] Ohio and Arkansas recently enacted legislation that would implement online parental consent and age verification 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. The fate of a similar law in Utah is also in jeopardy as it is also facing legal challenges.[14] 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 the concerns of the sponsor and the Senate Commerce and Technology Committee 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

[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. Griffin* (W.D. Ark. 5:23-cv-05105); *NetChoice, LLC v. Yost* (S.D. Ohio 2:24-cv-00047); *NetChoice, LLC v. Reyes* (D. Utah 2:23-cv-00911); *Zoulek et al. v. Hass & Reyes* (D. Utah 2:24-cv-00031).