June 15, 2023

Assembly Committee on Judiciary
Legislative Office Building
1020 N Street, Room 104
Sacramento, CA 95814

RE: SB 680 - "Features that harm child users: civil penalty" (Oppose)

Dear Chair Maienschein and Members of the Assembly Committee on Judiciary:

On behalf of the Computer & Communications Industry Association (CCIA), I write to express our respectful opposition to SB 680.

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 our members. CCIA also 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.[2] CCIA's members have been leading the effort in raising the standard 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.

CCIA has several concerns with SB 680's provisions as it is currently drafted which are further detailed in the following comments.

1. California should not impede continuing efforts by private businesses to effectively moderate content on their services, including through the use of algorithms.

The bill's requirements for the removal of content are undefined and difficult for businesses to comply with. Just as digital services do not serve all users, they do not publish all content. In addition to prohibiting illegal content as required by relevant state and federal laws, many digital services remove content that is dangerous, though not inherently illegal. This includes, for example, content that exhorts users to self-harm or encourages young people to engage in dangerous or destructive behavior.

Setting aside the matter of whether the government should impose upon private companies the obligation to host or take down lawful speech, which may raise First Amendment concerns, digital services are already taking aggressive steps to moderate and remove dangerous and illegal content consistent with their terms of service. The companies deliver on the commitments made to their user communities with a mix of automated tools and human review. In 2021, a number of online businesses announced that they have been voluntarily participating in the Digital Trust & Safety Partnership (DTSP) to develop and implement best practices 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/.

ensure a safer and more trustworthy internet, and have recently reported on the continuing efforts to implement and strengthen these commitments.[3]

As U.S. federal law limits the liability of both digital service providers and their users with regard to content created by third parties, this is a subject of ongoing federal attention. Recently, the U.S. Supreme Court declined to recommend any changes to a key tenet of U.S. Internet law in *Gonzalez v. Google*,[4] in which the Court was considering issues related to content moderation and organization methods. CCIA recommends pausing this proposal until legislators can act with fuller knowledge of the constitutional boundaries. Otherwise, any potential statute may be at greater risk of protracted, expensive litigation.

2. The bill lacks narrowly tailored definitions.

As currently written, the bill does not provide specific definitions that are necessary for businesses to comply. For example, "exercise of reasonable care" is not defined in this bill. Without knowing what the standard is for "reasonable care," businesses will struggle to ensure that non-content does not reach a child user.

Further, terms such as "addiction" lack adequate scientific foundation. In the absence of any medical consensus on the topic, private businesses will not be able to coherently or consistently make diagnostic assessments of users. It is also very difficult to reliably describe what may "cause physical, mental, emotional, developmental, or material harm" to a child user. Human beings in general, especially children, have very nuanced opinions surrounding what may be harmful to them. The lived experiences of children, teens, and adults differ immensely, and businesses do not have a roadmap to users' lived experiences, and what could potentially cause them harm. For example, based on videos a teenager viewed regarding current international events and global affairs, a digital service may recommend other videos about the war in Ukraine to a 17-year-old, but those videos could include depictions of bombings and death that could negatively affect or "harm" that user emotionally.

The lack of narrowly tailored definitions could create an incentive to simply prohibit minors from using digital services rather than face potential legal action and hefty fines for non-compliance. Consequently, this law could produce barriers for young adults using the internet for education or expression purposes, and inhibit their ability to learn how to navigate the internet while maturing their digital skills. Such skills are key to the personal and professional success of many adults in a society that increasingly relies on and uses digitally connected services.

CCIA believes an alternative to solving these complex issues is to work with private businesses to continue their ongoing private efforts to implement mechanisms such as daily time limits or child-safe searching so that parents can have control over their own child's social media use. 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 are already out there that they can use now to protect their children the way they see fit and based on their family's lived experiences.[5]

[3] 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.
[4] Trevor Wagener, *A Ruling Against Google in Gonzalez Could Create a "World of Lawsuits" and "Economic Dislocation,"* Disruptive Competition Project, (Feb. 27, 2023), https://www.project-disco.org/competition/gonzalez-v-google-could-create-a-world-of-lawsuits-and-economic-dislocation/.
[5] *See supra* note 2.

3. New regulations would impose duplicative responsibilities on businesses without tangible consumer benefits.

SB 680 would require companies to compile and submit quarterly audits of their designs, algorithms, and features. Many online platforms already voluntarily and regularly generate such reports and make them publicly available on their websites. Doing so is in fact an evolving industry practice: since its launch, DTSP has quickly developed and executed initial assessments of how its member companies are implementing the DTSP Best Practices Framework, which provides a roadmap to meaningfully increase trust and safety online. This roadmap includes several commitments to transparency and content moderation disclosures, in addition to others, to which DTSP members are expected to adhere.[6]

However, the development of such reports is extremely labor-intensive, and requiring detailed documentation with this frequency could disproportionately burden smaller companies with limited resources. CCIA recommends that the auditing and reporting requirement be limited to annually instead of quarterly to offset the time and labor necessary to produce such detailed reports.

Further, SB 680 does not detail to whom these audits would be submitted. The designs, algorithms, and features that would be required to be disclosed under this bill are considered proprietary information, containing trade secrets and other kinds of intellectual property. Without a further definition of who would be receiving these audits and how they would be maintained, provisions may be both overly prescriptive and counterproductive to the legislation's intended goals — rather than protecting consumers from harmful content, they might have the unintended adverse consequence of giving nefarious foreign agents, purveyors of harmful content, and other bad actors a playbook for circumventing digital services' safety mechanisms. CCIA recommends narrowing the type of information requested in audits and to whom this information is shared, such as limiting it to the state attorney general, to allow businesses to be more candid, avoid overburdening regulators and businesses, and protect potentially sensitive information.

4. Investing sole enforcement authority with the state attorney general and providing a cure period would be beneficial to consumers and businesses alike.

As currently written, the enforcement mechanism in SB 680 permits the Attorney General and various local prosecutors to bring legal action against companies that have been accused of violating new regulations.

By allowing for such a wide range of prosecutorial actions, this measure would invite speculative claims not rooted in science, with little evidence of actual injury. As lawsuits prove extremely costly and time-intensive for both the state and the litigants, it is foreseeable that these costs would ultimately be paid by taxpayers and individual users and advertisers in California, disproportionately impacting smaller businesses and startups across the state.[7] CCIA recommends establishing sole enforcement authority with the state attorney general to allow businesses time to consult with the AG's office to further course correct and come into compliance. This allows businesses to make the necessary changes and tailor those changes to what is best for the user.

---

[6] *See, e.g.*, DTSP, *The Safe Assessments: An Inaugural Evaluation of Trust & Safety Best Practices* at 37 (July 2022), https://dtspartnership.org/wp-content/uploads/2022/07/DTSP_Report_Safe_Assessments.pdf (Appendix III: Links to Publicly Available Company Resources).

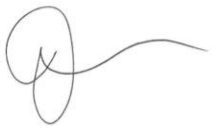
[7] Trevor Wagener, *State Regulation of Content Moderation Would Create Enormous Legal Costs for Platforms*, Broadband Breakfast (Mar. 23, 2021), https://broadbandbreakfast.com/2021/03/trevor-wagener-state-regulation-of-content-moderation-would-create-enormous-legal-costs-for-platforms/.

We also suggest providing a 30-day cure period to make sure digital services can consult with the Attorney General and come into compliance before incurring penalties. This would allow for actors operating in good faith to correct an unknowing or technical violation, reserving formal lawsuits and violation penalties for the bad actors that the bill intends to address. This would also focus the government's limited resources on enforcing the law's provisions for those that persist in violations despite being made aware of such alleged violations. Such notice allows consumers to receive injunctive relief but without the time and expense of bringing a formal suit. Businesses would also be better equipped with the time and resources to address potential changes rather than shifting focus to defending against litigation.

* * * * *

While we share the Committee's concern regarding the potential impact the internet may have on children, we encourage lawmakers to resist advancing legislation that is not adequately tailored to this objective. 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

CC: Senator Nancy Skinner
Suite 8630, State Capitol
1021 O Street
Sacramento, CA 95814-4900