April 18, 2023

Senate Committee on Judiciary
Attn: Christian Kurpiewski, Committee Counsel
1021 O Street
Sacramento, CA 95814

RE: SB 845 - "Let Parents Choose Protection Act of 2023." (Oppose)

Dear Chair Umberg and Members of the Senate Committee on Judiciary:

On behalf of the Computer & Communications Industry Association (CCIA), I write to express our respectful opposition to SB 845.

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 845's provisions as it is currently drafted which are further detailed in our following comments.

1. The goal of SB 845 can be accomplished with tools, preferences, and settings that are already available and do not require third-party applications.

Certain third-party software providers are now offering products aimed at addressing parents' concerns about their children's exposure to online harms such as cyberbullying or harassment. However, there are existing effective approaches that would not require the use of a third-party application. As previously mentioned, CCIA members have been leading efforts to incorporate additional features, settings, and preferences that allow parents to have more control over and insight into the activities their children are participating in online. We provide several examples of these tools below, however, this is not an exhaustive list.

Consumers may choose to use Domain Name System (DNS) servers to further customize and secure the online experience for their household.[3] Such servers include free options that allow a consumer to block certain websites and filter content to prevent younger users from accessing or viewing undesirable and other materials a particular parent deems as inappropriate or risky for their child.

[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] Mike Williams, *Best free and public DNS servers of 2023*, TechRadar (Feb. 6, 2023), https://www.techradar.com/news/best-dns-server.

Similarly, certain routers are equipped with virtual private network (VPN) software that allows a consumer to restrict access to certain sites and content for the devices that connect to the router. Specific browsers that can be installed by a parent or legal guardian can also allow for similar customization of managing site and content access.

2. While the bill's intent is to provide further protections for younger users, the bill would create a range of privacy concerns.

SB 845 would effectively create a framework under which a third-party vendor would be able to amass a significant amount of personal information about users under 18 across many service types. This creating and storing of such a vast amount of data by a vendor about this younger population inherently raises concerns about the security practices of those third-party vendors.

The bill also raises security concerns with regard to requiring private companies to make their APIs accessible to third parties. Generally, application programming interfaces (APIs) that are maintained internally are subject to a greater level of protection, through several layers of security. Opening up the level of accessibility would pose additional risks.

For example, employing such tools could be abused by parents who overly restrict a child's access to information. LGBTQ+ youth could be subject to additional restrictions in connecting with like-minded individuals, particularly in households where their parents or guardians may not support or agree with their orientation. Similarly, a teen could be seeking reproductive health resources when they do not feel comfortable having such important and consequential conversations with their parents or guardians. Or, a child could be living in an abusive or otherwise unsafe household and using additional measures to track and monitor that child could allow an abuser to exert additional control and harmful restrictions.

Recent studies have also sparked concerns at the federal level. In 2021, Senators Elizabeth Warren (D-MA), Edward J. Markey (D-MA), and Richard Blumenthal (D-CT) submitted a letter to the Chief Executive Officer of Bark Technologies, Inc., outlining significant concerns about how the software may be "surveilling students inappropriately" and "compounding racial disparities in school discipline".[4] While the letter focuses on negative impacts of using such "surveillance" software in an educational setting, the concerns extend beyond that – it boils down to the fundamental issue that this third-party software allows for the tracking and surreptitious control of nearly all of a child's online behavior. As we detail later in our comments, this could disproportionately affect younger users in certain minority communities and populations.

3. SB 845 introduces concerns regarding equity and accessibility, and does not provide how penalties for those who do not abide by the law will be enforced.

As currently written, SB 845 would require some form of age estimation or verification to provide parental access to third-party monitoring options. However, it is unclear in SB 845 what impact the use of VPNs to evade state-specific requirements by users could have on organizations' liability under this bill. It is also unclear if those who evade age verification or parental consent requirements would

[4] Letter from Senators Warren, Markey, and Blumenthal to Brian Bason, CEO of Bark Technologies (Sept. 29, 2021), https://www.warren.senate.gov/imo/media/doc/2021.09.29%20Bason%20-%20EdTech%20letter.pdf.

be held liable for breaking this potential law or if that liability would be incurred by the "large social media platform."

Serious concerns also arise when verifying whether a "parent" 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" is actually a minor's legal parent or guardian, this may incentivize minors to ask other adults that 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.

4. SB 845 would impose significant and potentially infeasible compliance burdens on businesses.

SB 845 would require "large social media platforms" to build an API to permit and allow a third-party provider to carry out a defined list of activities. While this may seem to be a simple exercise, to comply with such an effort would require significant labor and other resources. This is, in part, due to the particular complexities involved with the management of content and account settings, particularly at the granular levels that would be targeted under SB 845. In order for businesses to comply and remain compliant with the API requirements, the cost would be sizable. As every social media platform operates differently, it would also be challenging to consider an interface that would be able to manage all the granular details of a child's account, especially when an account performs different functions across different platforms.

In addition, once an API is published, third-party software providers would rely on that API, which in turn would limit the ability of the private company to innovate on their product where those innovations might require changes to the API. The bill appears to require that once an API is made available, it continues to be made available, limiting the ability to update and improve these interfaces over time. As just one example, the APIs for email were set early in the life of the internet and did not include provisions for control of spam and for end-to-end encryption. The inability to update the API for email has made these features effectively impossible to implement, even while they are trivially implementable in products with APIs that are either private or subject to change without restriction.[5]

[5] *Cf.* Moxie Marlinspike, *Reflections: the ecosystem is moving* (May 10, 2016), https://signal.org/blog/the-ecosystem-is-moving/.

* * * * *

While we share the concerns of the sponsor and the 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,

Khara Boender
State Policy Director
Computer & Communications Industry Association

CC: Senator Henry Stern
Attn: Rachel Buller, Legislative Aide
State Capitol
Suite 7710, 1021 O Street
Sacramento, CA 95814-4900