March 13, 2024

Re: Business Community Concerns with SB 780 - "Internet-Connected Devices and Internet Service Providers - Default Filtering of Obscene Content (Maryland Online Child Protection Act)"

Dear Chair Beidle and Members of the Senate Finance Committee,

Children deserve enhanced security and privacy online. We appreciate your work on protecting children and providing them with a safe online environment. The business community takes seriously the shared responsibility of incorporating robust protective features in their devices, websites, services, and platforms.[1] While we support the underlying intent of keeping young people safer online, the above five undersigned organizations[2] have serious concerns that requiring a state-specific default filter is not adequately tailored to this objective. While this bill diverges from proposals seen in other states, such as Idaho, Iowa, and Utah, by specifying that the requirements would apply to a 'device that is marketed toward or primarily sold for the use of individuals under the age of 18 years,' concerns surrounding technical feasibility remain.

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. Imposing a state-specific default filter is technologically infeasible and would create unobtainable expectations concerning content that filters can reasonably block. Additionally, internet-connected devices cannot activate filters and other protective features within the confines of a single state, let alone adapt as the device is transported across state borders. As such, we respectfully urge you to oppose the passage of this bill and appreciate the opportunity to further expand on our concerns with the proposed legislation.

---

[1] Competitive Enterprise Institute, *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/.
[2] The business community expressed these and a variety of other concerns in letters in current and past state sessions. *See* Letters from ACT | The App Association, CCIA, and TechNet Re: Concerns with Device Filter Proposals, *available at* https://actonline.org/wp-content/uploads/020524_ACT_Opposition_-SB_1253.pdf, *available at* https://ccianet.org/news/2024/02/ccia-testifies-submits-comments-on-device-filtering-bills-in-iowa-idaho/, *available at* *https://www.technet.org/wp-content/uploads/2024/02/AZ-HB-2661-Toma-Device-Filter.pdf*.

Currently, there are many different filter technologies in a robust and competitive marketplace that provide individuals, families, and commercial entities with a wide range of choices, quality, and cost. Mandating that a device activate a 'filter' undermines competition for competing products and ignores the different approaches to providing effective protection for networks, devices, and individual applications. Additionally, 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. 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. These types of filters and settings, however, are not activated by default. For example, the bill includes 'an internet-connected gaming device' under the bill’s definition of 'device intended for minors.' This definition could encompass a wide range of products, including those that are commonly used by adult users. SB 780 could invite significant consumer confusion for adults who are not aware that such filters aimed for children are set by default. We 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.

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, this proposal gives rise to substantial liability concerns stemming from the subjective interpretation of what qualifies as 'material that is harmful to minors.' Given diverse individual and community perceptions, there exists a considerable risk of legal liability for companies that struggle to adhere to dynamic and subjective norms, particularly when a device moves across state boundaries. Implementing these subjective requirements lacks technological feasibility.

The business community advocates for alternative approaches to safeguarding children online such as California’s recently passed 2023 AB 873. This legislation requires the Instructional Quality Commission to incorporate media literacy content at each grade level, including media literacy content into mathematics, science, and history-social science curriculum frameworks. We urge lawmakers to consider following a framework similar to California’s law and refrain

from passing alternative regulations until laws like California's have been thoroughly implemented, allowing for a more informed assessment of the success of these programs.

Moreover, promoting online safety campaigns like CTIA's Mobile Parent[3] or SIIA's Keep Kids Safe and Connected[4] provides an additional avenue for enhancing safety for children online. This offers parents a convenient and readily accessible method to promptly access and implement recommended safety measures in their homes. Both of these approaches avoid imposing a technologically and operationally infeasible law. In lieu of such legislation, states should explore narrowly tailored, risk-based strategies for crafting protections customized to various age groups and concentrate on addressing tangible harms.

While we have concerns about SB 780, we are committed to working to ensure that children's online safety concerns are appropriately addressed and hope to work with members of the Legislature on this important and complicated matter.

Sincerely,

ACT | The App Association
Computer & Communications Industry Association
Consumer Technology Association
TechNet
Software & Information Industry Association (SIIA)

[3] CTIA-The Wireless Association, *Mobile Parent*, https://mobileparent.org/.
[4] Software and Information Industry Association (SIIA), *Keep Kids Safe and Connected*, https://www.keepkidssafeandconnected.com/.