February 5, 2024

Senate State Affairs Committee
P.O. Box 83720
Boise, ID 83720-0081

RE: SB 1253 - Children's Device Protection Act. (Oppose)

Dear Chair Guthrie and Members of the Senate State Affairs Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SB 1253.

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.

Acknowledging policymakers' valid concerns about the online privacy of young individuals, it is imperative to prioritize the establishment of a comprehensive data privacy law applicable to all consumers. This law should incorporate safeguards for sensitive data, specifically addressing information commonly linked to younger users.

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]

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

[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.

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.

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 to manage and restrict access to certain content.

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. 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.

Additionally, a thriving market currently exists in the realm of online content filters for devices designed for commercial use, a choice embraced by numerous schools. Beyond that, many school districts may opt for additional commercial solutions to enhance their content filtering capabilities. This includes solutions that are installed at the network level that manage what content students can and cannot access while on a school provided network. The decision to use these types of filters at the device and network level is a choice between administrators and parents free of any need of state government intervention or regulation.

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.

2. 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 are able to see and use[5]. These types of filters and settings, however, are not activated by default. SB 1253 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.

3. 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 1253 gives rise to substantial liability concerns stemming from the subjective interpretation of what qualifies as "obscene material" or "harmful content." 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.

* * * *

CCIA advocates for alternative approaches to safeguarding children online such as Florida's recently passed SB 104. This legislation facilitates comprehensive training on internet and social media safety for students, parents, and teachers across the entire state. CCIA urges lawmakers to consider following a framework similar to Florida's law, and refrain from passing alternative regulations until laws like Florida'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 mobileparent.org 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. To prevent the enactment of such legislation, states should explore narrowly tailored, risk-based strategies for crafting protections tailored to various age groups and concentrate on addressing tangible harms.

We appreciate your consideration of these comments and stand ready to provide additional information as the Legislature considers proposals related to technology policy.

Sincerely,

Khara Boender

[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/\.

State Policy Director
Computer & Communications Industry Association