January 23, 2024

Senate Committee on Judiciary, Law Enforcement, and Criminal Justice
Attn: Lacey Johnson, Policy Analyst
Suite 320, State Capitol
350 North State Street
Salt Lake City, UT 84114

Re: SB 104 - Children's Device Protection Act (Oppose)

Dear Chair Weiler and Members of the Senate Committee on Judiciary, Law Enforcement and Criminal Justice:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SB 104.

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]

---

[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.

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.

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.

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 provides users with a wide range of choices, quality, and cost. Mandating that a device activate an "obscenity 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, 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 are able to see and use[5]. These types of filters and settings, however, are not activated by default. SB 104 could invite

[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/\.

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.

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 104 creates significant liability concerns due to the subjective nature of what may be considered "obscenity" or "harmful to a minor". 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 is technologically implausible. This subjectivity especially raises concerns for businesses particularly with the threat of lawsuits under the bill's private right of action.

SB 104 permits consumers to bring legal action against businesses that have been accused of violating new regulations. By creating a new private right of action, the measure would open the doors of SB 104's courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. Lawsuits also prove extremely costly and time-intensive – it is foreseeable that these costs would be passed on to individual consumers in Utah, disproportionately impacting smaller businesses and startups across the state. Further, investing enforcement authority with the state attorney general allows for the leveraging of technical expertise concerning enforcement authority, placing public interest at the forefront.

* * * *

CCIA recommends alternative approaches to protecting children, including proposals to include educational curricula focused on how to be a good citizen online. Promoting online safety campaigns, such as CTIA's Mobileparent.org, is another means to improve safety. And to avoid imposing a technologically and operationally infeasible law, states could consider narrowly-tailored, risk-based approaches to developing protections for different ages of users and by focusing on 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
State Policy Director
Computer & Communications Industry Association