February 3, 2025

House Judiciary Committee
Artificial Intelligence, Cybersecurity, & Special Laws Subcommittee
Post Office Box 11867
Columbia, South Carolina 29211

Re: HB 3399 - "Children's Default to Safety Act" (Oppose)

Dear Chair Moore and Members of the House Judiciary Committee Artificial Intelligence, Cybersecurity, & Special Laws Subcommittee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 3399 in advance of the House Judiciary Committee Artificial Intelligence, Cybersecurity, & Special Laws Subcommittee hearing on February 4, 2025. 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. Recent sessions have seen an increasing volume of state legislation related to the regulation of what digital services host and how they host it. While recognizing that policymakers are appropriately interested in the digital services that make a growing contribution to the U.S. economy, these bills require study, as they may raise constitutional concerns, conflict with federal law, and risk impeding digital services in their efforts to appropriately manage content.

CCIA 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 children's 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.

However, requiring a state-specific default filter would present significant technical difficulties for businesses. Typically, internet service providers (ISPs) govern which websites users can access. For example, known rogue sites are blocked by ISPs, not the manufacturer who produces the devices. It is also important to consider how the bill's provisions would apply to devices that do not have precise location-tracking technology or only connect via WiFi. Similarly, the bill raises questions surrounding how to account for devices purchased online from an out-of-state location, or for devices purchased on the secondary market. While it is easier to determine whether a device is activated in the state based on point of sale, the myriad options available to consumers to purchase devices from outside of South Carolina raise significant questions about how the bill's provisions would apply. We appreciate the opportunity to further expand on our concerns with the proposed legislation.

[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://project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/.

A mandatory device filter would remove a user's individual ability to tailor preferences regarding content and services.

Mandating that a device activate a 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. These types of filters and settings, however, are not activated by default. HB 3399 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 continues to be voluntary and that such features be opt-in for the specific consumers who wish to utilize them.

Age verification requirements raise significant privacy concerns.

The bill inherently requires age verification, given that it applies to filters for users that are under the age of 18. Under this bill, age verification would occur at the point of sale, but for devices that are sold on the secondary market or outside of South Carolina's borders, age verification would need to occur at separate points in a device's lifecycle.

Determining a user's age inherently requires collecting additional, sensitive data from users. If the state were to force companies to collect more user data even as others are requiring the collection of less data, it may place businesses in an untenable position of picking which state's law to comply with, and which to unintentionally violate.[3]

Additionally, age verification solely at the device operating system or application store level overlooks access to websites via desktop or other devices. Numerous applications are designed for use through a browser, which this method does not cover. While it might seem like a comprehensive solution to regulating access to certain content deemed undesirable for younger users, in reality, it falls short of achieving that goal.

A recent study from the Pew Research Center found that many Americans worry about children's online privacy but when asked about who is responsible for protecting children's online privacy, most (85%) say parents hold a great deal of responsibility for protecting kids' online privacy. 59% also say that tech companies bear the responsibility, while 46% believe the government does. The study also highlights why it is important to consider the trade-offs associated with age verification and related proposals that would require the additional

[3] Caitlin Dewey, *California's New Child Privacy Law Could Become National Standard*, The Pew Charitable Trusts (Nov. 7, 2022), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/11/07/californias-new-child-privacy-law-could-become-national-standard.

collection of data; around 89% of Americans are very or somewhat concerned about social media platforms knowing personal information about kids.[4]

Further, the Commission Nationale de l'Informatique et des Libertés (CNIL) analyzed several existing online age verification solutions but found that none of these options could satisfactorily meet three key standards: 1) providing sufficiently reliable verification; 2) allowing for complete coverage of the population; and 3) respecting the protection of individuals' data, privacy, and security.[5] Though the intention to keep kids safe online is commendable, this bill is counterproductive to that initiative by requiring more data collection about young people.

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, HB 3399 creates significant liability concerns due to the subjective nature of what may be considered "harmful to minors", as defined in Section 16-15-375(1), including that it "lacks serious literary, artistic, political, or scientific value for minors". Standards for what is deemed to be art versus potentially lacking "serious literary, artistic, political, or scientific value" may be tied to different community and cultural norms that can vary considerably across small geographic areas. The notion that a device could accurately adapt to these dynamic and subjective norms as it is moved about is implausible and certain to result in over-filtering. This subjectivity especially raises concerns for businesses particularly with the threat of lawsuits under the bill's private right of action, as further detailed below.

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

HB 3399 permits consumers to bring legal action against individuals and businesses that have been accused of violating new regulations. By creating a new private right of action, the measure would open the doors of South Carolina's courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. The bill explicitly does not preclude class action lawsuits and includes a cause of action against individual persons that could be weaponized in family court or disputes between co-parents. Lawsuits prove extremely costly and time-intensive — it is foreseeable that these costs would be passed on to individual consumers in South Carolina, disproportionately impacting smaller businesses and startups across the state. Further, investing sole enforcement authority with the state attorney general allows for

[4] Colleen McClain, *How Americans View Data Privacy*, Pew Research Center: Internet, Science & Tech (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.
[5] *Online age verification: Balancing Privacy and the Protection of Minors,* CNIL (Sept. 22, 2022), https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.

the leveraging of technical expertise concerning enforcement authority, placing public interest at the forefront.

CCIA also recommends that the legislation include a cure period of at least 30 days. 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. It 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.

* * * * *

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,

Megan Stokes
State Policy Director
Computer & Communications Industry Association