



March 11, 2025

Senate State Affairs Committee
Attn: Kathryn Wells
P.O. Box 83720
Boise, ID 83720-0081

Re: S. 1158 – "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 S. 1158 in advance of the Senate State Affairs Committee hearing on March 12, 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.

CCIA firmly believes that children are entitled to greater security and privacy online. Our members have designed and developed settings and parental tools to individually tailor younger users' online use to their developmental needs. For example, various services allow parents to set time limits, provide enhanced privacy protections by default for known child users, and other tools allow parents to block specific sites entirely.² This is also why CCIA supports implementing digital citizenship curricula in schools, to not only educate children on proper social media use but also help teach parents how they can use existing mechanisms and tools to protect their children as they see fit.³ However, this bill presents the following concerns:

S. 1158 does not fairly or consistently regulate many common devices.

Requiring a state-specific default filter "preventing the device from accessing or displaying obscene material as defined by state law through internet browsers or search engines owned or controlled by the manufacturer" would present significant technical difficulties for businesses. Typically, internet service providers (ISPs) govern which websites users can access. ISPs block known rogue sites, not the device's manufacturer.

Moreover, many devices could not be regulated in a consistent or fair manner under such a bill, including devices that do not have precise location-tracking technology or only connect via WiFi. Similarly, the bill fails 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

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 Competitive Enterprise Institute, *Children Online Safety Tools*, <https://cei.org/children-online-safety-tools/> (last updated Feb. 19, 2025).

³ 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/>.



whether a device is activated in the state based on point of sale, the bill provides no consistent means of regulating devices purchased outside of Idaho.

A mandatory device filter would curtail individuals' ability to tailor their preferences regarding content and services, including adults.

It is possible to protect children online without a statewide device filter. Many products, both digital and physical, can have effective child safety features installed on them even if they are primarily designed for adults. For example, automobiles are designed with seats and seatbelts for adult consumers. However, parents can install car seats designed specifically for children's safety. Likewise, many devices and services have content filtering technologies that allow parents to individually tailor settings and preferences to select age-appropriate content for themselves and their children. These types of filters and settings, however, are not activated by default. S. 1158 could invite significant consumer confusion for adults who are unaware that such filters geared toward minors are activated automatically. CCIA recommends allowing consumers to activate such features voluntarily using an opt-in feature.

The bill's safe harbor could lead to even broader restrictions, as it applies only to manufacturers that make a "good faith effort" to provide a device that, upon activation in Idaho, "automatically enables a generally accepted and commercially reasonable filter that blocks obscene material on all internet browsers and search engines accessed on the device". This could mean devices activated in Idaho automatically have such a filter, even adults'.

The bill's provisions harm businesses operating online, who depend on clear regulatory certainty across jurisdictions nationwide, and their users.

Ambiguous and inconsistent regulation at the state or local levels undermines business certainty, creating significant confusion surrounding compliance. This type of regulatory balkanization may deter new entrants, harming competition, innovation, and consumers. Devices sold into a national market are not and cannot be designed to function differently merely because they have moved within a state's borders.

Further, S. 1158 creates significant liability concerns due to the subjective nature of what may be considered "harmful" or "obscene." S. 1158's "declaration of policy" mentions "pornographic content that is harmful," while the rest of the bill uses the term "obscene material." There is no systematic, objective way to differentiate obscenity from protected speech; such determinations must instead be made on a case-by-case basis, as Idaho law appears to acknowledge.⁴ Covered entities cannot be expected to make such subjective assessments, and will inevitably engage in over-filtering to ensure compliance. Requiring businesses to make such subjective assessments is especially risky given the bill's penalties of \$5,000 per violation, capped at \$50,000 in aggregate in any specific case, as well as injunctive relief, reasonable expenses, investigative costs, attorney's fees, and "other appropriate relief."

⁴ S. 1158 points to Idaho Code § 18-4101 for the definition of "obscene material," which appears to be based on *Miller v. California*, 413 U.S. 15, 24 (1973).



Age determination requirements for online businesses are currently being litigated in several jurisdictions.

When the federal Communications Decency Act was passed, there was an effort to sort the online population into children and adults for different regulatory treatment. That requirement was struck down by the U.S. Supreme Court as unconstitutional because of the infeasibility.⁵ After 25 years, age authentication still remains a vexing technical and social challenge.⁶

Recent state legislation that would implement online age verification or estimation measures is currently facing numerous constitutional challenges, and numerous federal judges have placed laws on hold until these challenges can be fully reviewed, including in Arkansas, California, Mississippi, Ohio, Tennessee, Texas, and Utah.⁷ CCIA anticipates that these forthcoming rulings may clarify which age determination requirements are Constitutionally permissible. CCIA therefore recommends that lawmakers permit this issue to be more fully examined by the judiciary before burdening businesses with legislation that risks being invalidated and passing on expensive litigation costs to Idaho taxpayers.

* * * * *

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,

Aodhan Downey
State Policy Manager, West
Computer & Communications Industry Association

⁵ *Reno v. ACLU*, 521 U.S. 844, 855-57, 862 (1997).

⁶ Jackie Snow, *Why Age Verification Is So Difficult for Websites*, Wall St. J. (Feb. 27, 2022), <https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728>.

⁷ See, e.g., *NetChoice v. Bonta*, No. 24-cv-07885, 2025 WL 28610 (N.D. Cal. Jan. 2, 2025); *NetChoice v. Bonta*, No. 22-cv-08861, 2024 WL 5264045 (N.D. Cal. Dec. 31, 2024); *NetChoice, LLC v. Reyes*, No. 23-cv-00911, 2024 WL 4135626 (D. Utah Sept. 10, 2024); *NetChoice, LLC v. Fitch*, No. 24-cv-00170, 2024 WL 3276409 (S.D. Miss. July 1, 2024); *NetChoice, LLC v. Yost*, 716 F. Supp. 3d 539 (S.D. Ohio 2024); *NetChoice, LLC v. Griffin*, No. 23-cv-05105, 2023 WL 5660155 (W.D. Ark. Aug. 31, 2023); *Comput. & Commc’ns Indus. Ass’n et al. v. Paxton*, No. 24-cv-00849, 2024 WL 4051786 (W.D. Tex. Aug. 30, 2024).