JOSH GREEN, M.D.
GOVERNOR

SYLVIA LUKE
LIEUTENANT GOVERNOR

EMPLOYEES' RETIREMENT SYSTEM
HAWAI'I EMPLOYER-UNION HEALTH BENEFITS TRUST FUND
OFFICE OF THE PUBLIC DEFENDER

STATE OF HAWAI'I
DEPARTMENT OF BUDGET AND FINANCE
Ka 'Oihana Mālama Mo'ohelu a Kālā
P.O. BOX 150
HONOLULU, HAWAI'I 96810-0150

LUIS P. SALAVERIA
DIRECTOR

SABRINA NASIR
DEPUTY DIRECTOR

ADMINISTRATIVE AND RESEARCH OFFICE
BUDGET, PROGRAM PLANNING AND MANAGEMENT DIVISION
FINANCIAL ADMINISTRATION DIVISION
OFFICE OF FEDERAL AWARDS MANAGEMENT

WRITTEN ONLY

TESTIMONY BY LUIS P. SALAVERIA
DIRECTOR, DEPARTMENT OF BUDGET AND FINANCE
TO THE SENATE COMMITTEES ON COMMERCE AND CONSUMER PROTECTION
AND LABOR AND TECHNOLOGY
ON
SENATE BILL NO. 2309

February 15, 2024
9:35 a.m.
Room 229 and Videoconference

RELATING TO ONLINE SAFETY FOR CHILDREN

The Department of Budget and Finance (B&F) offers comments on this bill.

Senate Bill (S.B.) No. 2309 adds a new chapter entitled "Hawai'i Age-Appropriate Design Code Act" to establish the Hawai'i Age-Appropriate Design Code to promote privacy protections for children and ensure that online products, services, or features likely to be accessed by children are designed in a way that recognizes the distinct needs of children at different age ranges by:

- Setting required and prohibited actions that covered businesses that provide an online service, product, or feature likely to be accessed by children shall or shall not take beginning July 1, 2025.
- Requiring covered businesses to complete a data protection impact assessment, to be protected as confidential information and exempt from public disclosure, for any online service, product, or feature likely to be accessed by children and offered to the public by July 1, 2025.

- Creating penalties for negligent and intentional violations of this chapter, which shall be collected in a civil action brought by the Attorney General (AG) on behalf of the State and deposited into the Consumer Privacy Special Fund (CPSF).
- Establishing the CPSF, to be administered by AG, into which shall be deposited all civil penalties, expenses, and attorney fees collected pursuant to this chapter; interest earned on moneys in the fund; and appropriations made by the Legislature.
- Establishing a children's data protection working group, to be administratively attached to AG and set to dissolve on June 30, 2030, and requiring a report on its findings and recommendations on best practices for implementation of this chapter, along with any proposed legislation, to the Legislature no later than 20 days prior to the convening of the 2025 Regular Session and every other odd-numbered year thereafter. The working group shall consist of AG and a Chief Information Officer, who shall serve as co-chair pro tempore until a chair and vice chair are elected by the working group; the Director of the Office of Consumer Protection; and eight appointed or invited members.

As a matter of general policy, B&F does not support the creation of any special fund which does not meet the requirements of Section 37-52.3, HRS. Special funds should: 1) serve a need as demonstrated by the purpose, scope of work, and an explanation why the program cannot be implemented successfully under the general fund appropriation process; 2) reflect a clear nexus between the benefits sought and charges made upon the users or beneficiaries or a clear link between the program and the sources of revenue; 3) provide an appropriate means of financing for the program or activity; and 4) demonstrate the capacity to be financially self-sustaining.

Regarding S.B. No. 2309, it is difficult to determine whether the proposed special fund would be self-sustaining, especially given that this bill does not provide an appropriation to seed the newly created special fund until penalties can start being collected for violations of provisions that begin July 1, 2025.

B&F defers to AG regarding the operational impacts of this bill on the department.

Thank you for your consideration of our comments.

TESTIMONY OF
THE DEPARTMENT OF THE ATTORNEY GENERAL
KA ʻOIHANA O KA LOIO KUHINA
THIRTY-SECOND LEGISLATURE, 2024

ON THE FOLLOWING MEASURE:
S.B. NO. 2309, RELATING TO ONLINE SAFETY FOR CHILDREN.

BEFORE THE:
SENATE COMMITTEES ON COMMERCE AND CONSUMER PROTECTION AND ON LABOR AND TECHNOLOGY

DATE: Thursday, February 15, 2024 **TIME:** 9:35 a.m.

LOCATION: State Capitol, Room 229 and Videoconference

TESTIFIER(S): Anne E. Lopez, Attorney General, or
Christopher T. Han or Bryan C. Yee, Deputy Attorneys General

Chairs Keohokalole and Aquino and Members of the Committees:

The Department of the Attorney General provides the following comments on this bill.

This bill establishes the Hawaiʻi Age-Appropriate Design Code to promote privacy protections for children and ensure that online products, services, or features that are likely to be accessed by children are designed appropriately. This bill also establishes a Children's Data Protection Working Group, administratively attached to the Department of the Attorney General, to assess and develop recommendations on the best practices for the implementation of the Hawaiʻi Age-Appropriate Design Code. In addition, this bill establishes the Consumer Privacy Special Fund and penalties for violation of this act.

Our department has concerns as to the constitutionality of this bill. This bill appears to be modeled after the California Age-Appropriate Design Code Act (CAADCA), which is currently undergoing legal challenge. On September 18, 2023, the U.S. District Court for the Northern District of California issued a preliminary injunction enjoining California's Attorney General from enforcing CAADCA.

The District Court held that CAADCA likely infringes upon the First Amendment by regulating protected speech. The plaintiff in the case also raised claims under the Commerce Clause and federal preemption under the Children's Online Privacy

Protection Act and section 230 of the Communications Decency Act, although these issues have not yet been resolved by the District Court.

California appealed the ruling to the Ninth Circuit Court of Appeals, but a decision has not yet been issued. We believe that this bill presents the same constitutional concerns as CAADCA.

That said, these concerns would not affect the creation of a working group. However, as written, there are constitutional and legal concerns about the means of appointment of some of the members of the working group established by section -11 of the new chapter of the bill, at page 30, lines 18-21. The appointing authority for the executive branch working group should be the governor.

To resolve this issue, we recommend deleting the current paragraphs (5) through (7) of subsection (c) at page 30, line 18, through, page 31, line 2, and inserting new paragraphs (5) through (7) to read:

(5) Two members appointed by the governor from a list of nominees submitted by the president of the senate;

(6) Two members appointed by the governor from a list of nominees submitted by the speaker of the house of representatives; and

(7) Two members appointed by the governor from a list of nominees submitted by the attorney general.

The wording "or invited" should also be deleted from paragraph (4) at page 30, line 16.

Thank you for the opportunity to offer comments.

TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Southwest | Telephone 505.402.5738
915 L Street, Suite 1270, Sacramento, CA 95814
www.technet.org | @TechNetSW

February 13, 2024

Senator Jarrett Keohokalole
Chair, Committee on Commerce and Consumer Protection
Hawai'i State Capitol, Room 205
Honolulu, HI

Senator Henry Aquino
Chair, Committee on Labor and Technology
Hawai'i State Capitol, Room 204
Honolulu, HI

RE: SB 2309 (Elefante) – Age-Appropriate Design Code

Dear Chair Keohokalole, Chair Aquino, and Members of the Committee,

On behalf of TechNet's member companies, I respectfully submit this letter of opposition to SB 2309, regarding the age-appropriate design code.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over 4.2 million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance. TechNet has offices in Austin, Boston, Chicago, Denver, Harrisburg, Olympia, Sacramento, Silicon Valley, and Washington, D.C.

TechNet strongly believes children deserve a heightened level of security and privacy and there are several efforts within the industry to incorporate protective design features into their websites and platforms. Our companies have been at the forefront of raising the standard for teen 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. Our member companies are committed to providing a safe, age- appropriate experience for young people online; however, we are opposed to this bill's approach for several reasons.

The requirements in this bill would be difficult for our companies to implement. How these standards are enforced is deeply concerning, as there is little guidance, fewer opportunities to fix mistakes, and contains an aggressive approach to fines and penalties. This bill outlines requirements for business without illustrating the steps

to come into compliance. Additionally, this bill is preempted by the Children's Online Privacy Protection Act, or "COPPA". SB 2309 would change the threshold from COPPA's "directed to children" to "likely to be accessed by children". This is an overinclusive standard and would capture far more websites and platforms and subject them to this bill's requirements, which, as noted, are difficult to interpret and implement. Consideration should be given to websites, such as online news, which are likely to be accessed by users of all ages and do not require visitors to register to view content.

The requirement that companies consider the "best interests" of children is incredibly difficult to interpret. Different companies, even parents in one household, will have very different interpretations of what is and isn't in the "best interests" of children. In addition, the requirement that personal information cannot be used in a way that is demonstrably harmful to the physical, mental, or overall well-being of children is another example that is ambiguous. It's unclear who decides what is considered demonstrably harmful and how that determination is made. TechNet believes that parents and guardians should have smart choices so they can maintain the ultimate power to decide what is best for their children and families. As written, SB 2309 will impact parents' and guardians' rights to choose what types of content their children are able to access and could limit the ability of adult users to access member products and services. Given these stringent policies, this bill could very well limit access to important services or information for teens in the most vulnerable segments of the population including LGBTQ+ teens, teens in domestic abuse situations, and teens looking for reproductive health information.

SB 2309 would also require new standards for age verification. Age-verification is a complex challenge for our industry to address and requires consideration of how to properly balance the interests of privacy and security. Stringent age-verification would require the collection of more personal information such as birthdates, addresses, and government IDs. The standard in this bill would require companies to collect more personal information, which conflicts with data minimization principles. Efforts are ongoing to develop more privacy protective ways to verify age online. But until there are industry-wide tools available, age-verification will continue to have tradeoffs and be difficult to implement in practice. Unfortunately, no system is infallible.

California enacted the California Age-Appropriate Design Code Act in 2022 and it is substantially similar to SB 2309. The AADC would impact the structure and design of the Internet, ostensibly to protect minors, and would impose significant burdens on most online businesses. The law has a potentially sweeping impact on the entire internet.

The law is the subject of current litigation, with a district court granting a preliminary injunction and finding that the CA AADC likely violates the First and Fourth Amendments and the Dormant Commerce Clause, is unconstitutionally vague, and is preempted by COPPA and Section 230 of the Communications

Decency Act. Because of this pending litigation, TechNet recommends waiting until the litigation is concluded before considering similar legislation.

In conclusion, the best way to keep young people safe online is by promoting the education of safe internet practices. We support policies that help prepare young people to be a successful part of a global, interconnected, and technology-driven economy. Such policies include supporting digital learning resources and technology integration in student learning environments, fully funded K-12 education, and rigorous computer science standards. Digital citizenship education is a top priority for TechNet and its member companies. Several businesses participate in the Digital Trust & Safety Partnership (DTSP), which outlines best practices for those operating in the digital space. We would suggest that concerned stakeholders proactively partner with organizations and companies supporting digital citizenship and online safety education.

Additionally, we would suggest shifting the focus to an omnibus privacy solution. Other states' omnibus privacy laws cover children's data privacy and several other rights in comprehensive privacy laws, including rights to access, correct, port, and delete personal data. An omnibus privacy law to cover the protection of children online would provide for increased flexibility for businesses and citizens of Hawaii, as well as interoperability between states.

We recognize the importance of strong protections for youth, but those efforts should account for teens' autonomy and aim to achieve consistency with emerging norms. For the above stated reasons, including pending litigation, TechNet is opposed to SB 2309.

Thank you for your consideration. If you have any questions regarding our position please contact Dylan Hoffman, Executive Director, at dhoffman@technet.org or 505-402-5738.

Sincerely,

Dylan Hoffman
Executive Director for California and the Southwest
TechNet

CHAMBER OF PROGRESS

Testimony of Robert Singleton
Director of Policy and Public Affairs, US West
Chamber of Progress
Oppose SB 2309: Hawai'i Age-Appropriate Design Code

February 15, 2024

Dear Chairs Keohokalole, Aquino, and members of the Committees:

Thank you for the opportunity to submit testimony for the record regarding SB 2309. On behalf of the Chamber of Progress, a tech industry coalition promoting technology's progressive future, I urge you to **oppose** SB 2309 which would compromise online privacy and impose fundamental changes to how critical online services work, rendering many of them unusable for vulnerable populations in Maryland.

Our organization works to ensure that all Americans benefit from technological leaps. One of Chamber of Progress's top priorities is ensuring children have access to safe and inclusive online spaces. Unfortunately, many regulations and policies modeled after Age-Appropriate Design Code with the intention of protecting children may end up doing more harm than good by threatening privacy protections and exacerbating the vulnerabilities of marginalized young people.

Estimating age threatens online privacy
Age-Appropriate Design Code requires covered platforms to estimate the age of its users, whether through assumptions derived from the users' consumption of certain content, or through affirmative age verification methods. In either case, reliably ascertaining age - whether through inserting a birthdate, or uploading an ID, or even via biometric methods - is privacy-invasive and requires widespread data collection. Such techniques would have to be used for every user, not just children, resulting in increased data collection for everyone on the internet. This is contrary to the principle of data minimization.

Data Protection Impact Assessments are potentially litigiously cumbersome
For any website that is "likely to be accessed by children," SB 2309 requires a platform to create and deliver Data Protection Impact Assessments (DPIAs) each time the service creates a new service, product, or feature. Because all websites could be accessed by a

child and all websites carry a nonzero risk of harm to children, SB 2309's DPIA requirements effectively chill internet services from developing new products and features—even products and features that could materially benefit and improve safety for children—to avoid future litigation risks associated with their DPIAs.

There may be unintended consequences concerning the definition of "harm" to minors, including over-moderation.
The requirements as proposed in SB 2309 would require that covered platforms act in the "best interests" of child users and create a plan to "mitigate or eliminate" the risk of encountering "harmful, or potentially harmful, content," without providing clear guidance about what that entails.

While these are important considerations, in practice, this requirement would make each site the arbiter of appropriate content for children of all age ranges and circumstances. Platforms would face difficult choices about what types of content to consider "harmful", making content moderation even more complicated to implement.

Worse, this provision will cause social media platforms to avoid litigation by over moderating. This disproportionately impacts young people of color, as social media has provided a platform for teens and students of color to speak up against racial prejudice, with 82% of Black and Hispanic users stating that social media is effective for creating sustained social movements and preserving historically-marginalized groups' access to protected speech.

Fearful that the Attorney General may deem certain content "harmful" to some or all minors, or find a company's newly required child-centric data protection assessments inadequate, online services will be pressured to identify remote or unlikely harms—and to self-censor accordingly. The AADC will thus discourage websites from hosting and promoting content—for users under the age of 18 and for adults, due to age-assurance challenges—including critical resources that underprivileged children rely on to deal with familial and personal crises.

We agree with the need to build in greater protections for young users, but some of this bill's requirements would undermine the protections it tries to create and would end up harming vulnerable users.

CHAMBER OF PROGRESS

Accordingly, we encourage you to oppose SB 2309.

Thank you,

Robert Singleton
Director of Policy and Public Affairs, US West
Chamber of Progress

TESTIMONY OF TINA YAMAKI, PRESIDENT
RETAIL MERCHANTS OF HAWAII
FEBRUARY 15, 2024
SB 2309 RELATING TO ONLINE SAFETY FOR CHILDREN.

Good morning, Chair Senator Keohokalole and Chair Aquino and members of the Senate Committee on Commerce and Consumer Protection and the Senate Committee on Labor & Technology. I am Tina Yamaki, President of the Retail Merchants of Hawaii and I appreciate this opportunity to testify.

The Retail Merchants of Hawaii was founded in 1901, RMH is a statewide, not for profit trade organization committed to the growth and development of the retail industry in Hawaii. Our membership includes small mom & pop stores, large box stores, resellers, luxury retail, department stores, shopping malls, local, national, and international retailers, chains, and everyone in between.

We respectfully oppose SB 2309. This measure establishes the Hawai‘i Age-Appropriate Design Code to promote privacy protections for children and ensure that online products, services, or features that are likely to be accessed by children are designed in a manner that recognizes the distinct needs of children at different age ranges; establishes a Children's Data Protection Working Group, administratively attached to the Department of the Attorney General, to assess and develop recommendations on the best practices for the implementation of the Hawai‘i Age-Appropriate Design Code; and establishes the Consumer Privacy Special Fund. Establishes penalties.

Retailers like many businesses that have an online presence support protecting minors. However, it is our understanding that this **bill as currently written is taken from the California measure that was passed last year and was recently blocked by U.S. District Judge Beth Labson Freeman on the grounds that law's commercial speech restrictions likely violate the U.S. Constitution's First Amendment**. We wonder why the legislature would consider taking up a measure that could be challenged in Federal Court and not wait until more information and guidance is forthcoming once the Ninth Circuit issues its decision later this year.

We agree that companies should take steps to prevent harm to children, but it is important that those harms are defined in an actionable and specific way. The primary goal should be to specifically address the harms of social media on children. **We would like to point out that this area is already regulated by the FTC under the Children’s Online Privacy Protection Act, or COPPA, so that law already creates a floor or threshold as legislators think about imposing new laws that would apply just to Hawaii businesses and residents.**

But, **as drafted, the application of the Age-Appropriate Design Code (“AADC”) is sweeping – it encompasses the entire internet, applies to any website “likely to be accessed” by any minor under 18, and makes no distinction between a 7-year-old and a 17-year-old. This has the result of potentially impacting the products and services that are available to adults—not just children.** Examples include access to websites that provide information on abortion, gun rights and LGBTQ issues.

3610 Waialae Ave • Honolulu, HI 96816 (808) 592-4200 tyamaki@rmhawaii.org

Furthermore, the section in the bill that "materially detrimental to the physical health, mental health, or well-being of a child" is even more troublesome as it would require the operator to make that determination about content and impose liability if they do not. The court looking at this same language in the California bill held that it was overbroad and imposed an unconstitutional burden on businesses in seeking to require them to create and implement a "sliding scale of potential harms to children as they age", a standard that very few parents, businesses, legislators or even the AG could agree on. And it would create civil liability of up to $2,500 ($7,500 if the violation is "intentional") per child per each violation… a potentially huge monetary penalty for a failure to apply a vague and unworkable standard.

We also want to point out the ambiguities in the bill. As proposed a children's data protection work group in section 11 to provide guidance and put some better definitions around the obtuse and subjective terms throughout the bill. But the working group is after the fact. Perhaps it would be more appropriate to create the working group first, give it a charge and runway to examine the area, and then come back with recommendations on a bill that could be implemented by businesses for the benefit of Hawaii children and parents in a way that is more predictable, fair and even-handed.

Hawaii should be looking into passing a comprehensive privacy package that will provide adults, parents and their children privacy protections, clear and understandable guidance for companies, and laws that will withstand constitutional challenges.

We ask that you hold this measure. Mahalo for the opportunity to testify.

3610 Waialae Ave • Honolulu, HI 96816 (808) 592-4200 tyamaki@rmhawaii.org

February 15, 2024

LATE

Senate Committee on Commerce and Consumer Protection
Senate Committee on Labor and Technology
415 South Beretania Street
Honolulu, HI 96813

RE: SB 2309- "RELATING TO ONLINE SAFETY FOR CHILDREN." (Oppose)

Dear Chair Keohokalole, Chair Aquino, and Members of the Senate Committee on Commerce and Consumer Protection and Senate Committee on Labor and Technology:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SB 2309 in advance of the Joint Committee hearing on February 15, 2024.

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. 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. Presently, our members are actively engaged in various initiatives to integrate robust protective design features into their websites and platforms.[2] CCIA's members have been leading the effort to implement settings and parental tools to individually tailor younger users' online use to the content and services that are suited to their unique lived experience and 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 to allow parents to block specific sites entirely.[3]

This is also why CCIA supports the implementation of digital citizenship curriculum in schools, to not only educate children on proper social media use but also help educate parents on what mechanisms presently exist that they can use now to protect their children the way they see fit and based on their family's lived experiences.[4] In fact, the Hawaii Legislature is currently considering two proposals, HB 79 in the House and SB 914 in the Senate, that would advance informed digital citizenship in Hawaii's public education system by empowering school complexes to incorporate media literacy into standards-based curriculum.

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 disfavors. Proposals to keep children safe online should be established through a risk-based

[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.

approach to developing protections for different ages of users and by focusing on tangible harm. While CCIA shares the goal of increasing online safety, this bill presents the following concerns.

1. The bill lacks narrowly tailored definitions.

As currently written, the bill defines a child as anyone under 18. Due to the nuanced ways in which children under the age of 18 use the internet, it is imperative to appropriately tailor such treatments to respective age groups. For example, if a 16-year-old is conducting research for a school project, it is expected that they would come across, learn from, and discern from a wider array of materials than a 7-year-old on the internet playing video games. We suggest changing the definition of "child" to a user under the age of 13 to align with the federal Children's Online Privacy Protection Act (COPPA) standard. This would also allow for those over 13, who use the internet much differently than their younger peers, to continue to benefit from its resources. The definition of "likely to be accessed by children" is also ambiguous. CCIA recommends narrowly tailoring this definition to content intentionally targeted at or branded for children when they are using the internet.

The bill would also require businesses to provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using "clear language suited to the age of children likely to access that online service, product, or feature". The definition of "clear language suited to the age of children likely to access online services" is not defined and leaves room for significant subjective interpretation. If a child is defined as anyone under 18, one could expect a wide variation of reading comprehension skills across such a wide age group — a 17-year-old would presumably have better reading comprehension skills than that of a 5-year-old. Without "clear language" being defined, the bill would be difficult to comply with.

Additionally, this bill requires online businesses to "consider the best interests of children" when designing, developing, and providing an online service, product, or feature. The term "best interests of children" lacks a clear definition, leading to excessively vague requirements that prove challenging to implement on a large scale. This ambiguity creates moving goalposts for compliance, making it difficult to establish standardized operational criteria. The benefit of a dynamic marketplace is that online businesses are able to tailor their services and products to what is most relevant and useful to their specific audience. Private online businesses will not be able to coherently or consistently make diagnostic assessments of users, including their mental and physical health. Humans in general, especially children, have very nuanced opinions surrounding what may be harmful to them. The diverse lived experiences of children, teens, and adults vary significantly, leaving businesses without a comprehensive roadmap to navigate each user's unique perspective. Determining the optimal solutions for the well-being of each and every young individual engaging with an online platform poses a serious feasibility challenge.

2. The bill does not provide how a user's age will be estimated and how penalties for those who do not abide by the law will be enforced.

In order to achieve meaningful children's safety protections, it is imperative for businesses to have a roadmap of how to properly comply and avoid unintentional violations.[5] This measure provides broad strokes of *what* is expected of businesses but does not portend *how* businesses may achieve those objectives. Instead, businesses are expected to estimate ages with a "reasonable level of certainty" and "profile a child by default." CCIA suggests clarifying how businesses are expected to estimate the age of users online. Without a

[5] Digital Trust & Safety Partnership, *Age Assurance: Guiding Principles and Best Practices* (Sept. 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.

proper mechanism in place, it is difficult for businesses to discern the age of every individual user which could lead to unintended violations.

CCIA cautions against conflating concepts regarding estimating the age of users.[6] For example, when a website asks a user to make a self-attestation of their age, such as on a website for alcohol products, the owner of that website is not held liable if that user chooses to mischaracterize their identity. Similar self-attestation measures are currently in place for social media platforms and other digital services, and the burden is on the consumer to be forthcoming and honest about the age and birth date they enter. This, however, would change under SB 2309 — if online services were to rely on self-attestation for estimates but then in-turn be held liable for mischaracterizations, this would unreasonably treat the business as the bad actor. Further, it is unclear what impact the use of VPNs and similar mechanisms to evade state-specific age verification requirements by users could have on organizations' liability under this bill.

To achieve compliance and avoid the proposed penalties for violations, it is likely that age estimation would effectively amount to age verification. Current commercially available facial recognition and other mechanisms that provide age estimation cannot sufficiently accomplish what lawmakers are expecting.[7] The AADC purports not to require age verification, but the definitions and policy itself are so vague that sites will have no choice but to implement some kind of age verification technology to achieve compliance. Such verification requirements then raise questions about potential conflicts with data minimization principles and other consumer data privacy protection measures.

CCIA is concerned that businesses may be forced to collect age verification data, which would paradoxically force companies to collect a higher volume of data on children.[8] Businesses may be forced to collect personal information they don't want to collect and consumers don't want to give, and that data collection creates extra privacy and security risks for everyone. 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.[9] 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.

3. This bill may result in denying services to all users under 18. Limiting access to the internet for children curtails their First Amendment right to information accessibility, including access to supportive communities that may not be open discussion forums in their physical location.

The First Amendment, including the right to access information, is applicable to teens. Vague restrictions on protected speech cannot be justified in the name of "protecting" minor users online nor is a state legislative body the arbiter of what information is suitable for younger users to access. Moreover, when businesses are

[6] Khara Boender, *Children and Social Media: Differences and Dynamics Surrounding Age Attestation, Estimation, and Verification*, Disruptive Competition Project (May 10, 2023), https://www.project-disco.org/privacy/children-and-social-media-differences-and-dynamics-surrounding-age-attestation-estimation-and-verification.
[7] Berin Szóka, *Comments of TechFreedom In the Matter of Children's Online Privacy Protection Rule Proposed Parental Consent Method; Application of the ESRB Group for Approval of Parental Consent Method*, TechFreedom (Aug. 21, 2023), https://techfreedom.org/wp-content/uploads/2023/08/Childrens-Online-Privacy-Protection-Rule-Proposed-Parental-Consent-Method.pdf.
[8] Caitlin Dewey, *California's New Child Privacy Law Could Become National Standard*, The Pew Charitable Trusts (Nov. 7, 2022), https://pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/11/07/californias-new-child-privacy-law-could-become-national-standard.
[9] *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.

required to deny access to social networking sites or other online resources, this may also unintentionally restrict children's ability to access and connect with like-minded individuals and communities. For example, children of racial or other minority groups may not live in an area where they can easily connect with others that represent and relate to their own unique experiences. An online central meeting place where kids can share their experiences and find support can have positive impacts.

The hyperconnected nature of social media has led many to allege that online services may be negatively impacting teenagers' mental health. However, some researchers argue that this theory is not well supported by existing evidence and repeats a "moral panic" argument frequently associated with new technologies and new modes of communication. Instead, social media effects are nuanced,[10] small at best, reciprocal over time, and gender-specific. Additionally, a study conducted by researchers from Columbia University, the University of Rochester, the University of Oxford, and the University of Cambridge found that there is no evidence that associations between adolescents' digital technology engagement and mental health problems have increased.[11] Particularly, the study shows that depression's relation to both TV and social media was practically zero. The researchers also acknowledged that it is possible, for example, that as a given technology becomes adopted by most individuals in a group, even individuals who do not use that technology could become indirectly affected by it, either through its impacts on peers or by them being deprived of a novel communication platform in which social life now takes place.

4. Age estimation and verification requirements for online businesses are currently being litigated in several different 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.[12] After 25 years, age authentication still remains a vexing technical and social challenge.[13] California, Arkansas, and Ohio recently enacted legislation that would implement age verification and estimation requirements — each law is currently facing a legal challenge due to constitutional concerns, and judges recently put the laws on hold until these challenges can be fully reviewed.[14] The fate of a similar law in Utah is also in jeopardy as it is also facing legal challenges.[15] CCIA recommends that lawmakers permit this issue to be more fully examined by the judiciary in these ongoing challenges before burdening businesses with legislation that risks being invalidated or passing on expensive litigation costs to taxpayers.

5. Businesses operating online depend on clear regulatory certainty across jurisdictions nationwide.

Existing U.S. law provides websites and online businesses with legal and regulatory certainty that they will not be held liable for third-party content and conduct. By limiting the liability of digital services for misconduct by

[10] Amy Orben *et al.*, *Social Media's enduring effect on adolescent life satisfaction*, PNAS (May 6, 2019), https://www.pnas.org/doi/10.1073/pnas.1902058116.
[11] Amy Orben, Andrew K. Przybylski, Matti Vuorre, *There Is No Evidence That Associations Between Adolescents' Digital Technology Engagement and Mental Health Problems Have Increased*, Sage Journals (May 3, 2021), https://journals.sagepub.com/doi/10.1177/2167702621994549.
[12] *Reno v. ACLU*, 521 U.S. 844 (1997).
[13] Jackie Snow, *Why age verification is so difficult for websites*, The Wall Street Journal (Feb. 27, 2022), https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728.
[14] *NetChoice, LLC v. Bonta* (N.D. Cal. 5:22-cv-08861); *NetChoice, LLC v. Griffin* (W.D. Ark. 5:23-cv-05105); *NetChoice, LLC v. Yost* (S.D. Ohio 2:24-cv-00047); .
[15] *NetChoice, LLC v. Reyes* (D. Utah 2:23-cv-00911); *Zoulek et al. v. Hass & Reyes* (D. Utah 2:24-cv-00031).

third-party users, U.S. law has created a robust internet ecosystem where commerce, innovation, and free expression thrive — all while enabling providers to take creative and aggressive steps to fight online abuse. Ambiguous and inconsistent regulation at the state level would undermine this business certainty and deter new entrants, harming competition and consumers. This particularly applies to new small businesses that tend to operate with more limited resources and could be constrained by costs associated with compliance. While larger companies may be able to more easily absorb such costs, it could disproportionately prevent new smaller start-ups from entering the market.

Further, careful consideration of what constitutes best practice should consider inputs from practitioners and relevant stakeholders. Online businesses are already taking steps to ensure a safer and more trustworthy internet — recently, leading online businesses announced[16] that they have been voluntarily participating in the Digital Trust & Safety Partnership (DTSP) to develop and implement best practices and recently reported on the efforts to implement these commitments.[17] We urge lawmakers to study both the benefits and drawbacks of teen safety and privacy requirements and to engage with practitioners and stakeholders to support the ongoing development of practicable solutions.

6. In the United Kingdom, the Age Appropriate Design Code is not an enforceable law but is regulatory guidance for ensuring compliance with the UK Data Protection Act.

The Age Appropriate Design Code of the United Kingdom is not a law, but regulatory guidance, rooted in a UN Convention to which the United States does not belong. It is possible for a business to comply with UK law while not following the UK AADC. In fact, the UK Data Protection Act ("DPA") explicitly states that a "*failure by a person to act in accordance with a provision of a code issued under section 125(4) does not of itself make that person liable to legal proceedings in a court or tribunal.*"[18] The code was designed by the UK Information Commissioner's Office to meet its obligations under the UK DPA to prepare a code or suggestions for safe practice.

Many proponents of the Age Appropriate Design Code in the United States claim that the UK's internet is "still working." However, this mischaracterizes the approach taken in the United Kingdom. UK businesses processing personal data about UK children are not required to implement "*age estimations*" or other requirements in this proposed Act in order to operate. UK legislators avoided imposing "age verification" or similar higher thresholds upon organizations, recognizing the tension between higher accuracy and further data collection.

The UK also does not have the same fundamental and structural laws and rights that Americans do such as the Constitution and its First Amendment, nor does it share Americans' noted affinity for expensive civil litigation. Under U.S. law, where the proposed Act's language would be legally enforceable, covered entities would be forced to implement *age verification* measures to avoid potential liability — even if they did not want to direct their services to children.

---

[16] Margaret Harding McGill, *Tech giants list principles for handling harmful content*, Axios (Feb. 18, 2021), https://www.axios.com/techgiants-list-principles-for-handling-harmful-content-5c9cfba9-05bc-49ad-846a-baf01abf5976.html.
[17] *See, e.g.*, DTSP, *The Safe Assessments: An Inaugural Evaluation of Trust & Safety Best Practices* (July 2022), https://dtspartnership.org/wp-content/uploads/2022/07/DTSP_Report_Safe_Assessments.pdf (Appendix III: Links to Publicly Available Company Resources), at 37.
[18] *Age appropriate design: A code of practice for online services*, ICO (retrieved Mar. 2, 2023), https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/.

* * * * *

While we share the concerns of the sponsor and the members of the Committees regarding the safety of young people online, we encourage Committee members to resist advancing legislation that is not adequately tailored to this objective. 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,

Jordan Rodell
State Policy Manager
Computer & Communications Industry Association