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

LATE

ON THE FOLLOWING MEASURE:
S.B. NO. 2012, RELATING TO ONLINE PRIVACY FOR CHILDREN.

BEFORE THE:
SENATE COMMITTEES ON COMMERCE AND CONSUMER PROTECTION AND ON ENERGY, ECONOMIC DEVELOPMENT, AND TOURISM

DATE: Tuesday, February 13, 2024 **TIME:** 9:00 a.m.

LOCATION: State Capitol, Room 229 and Videoconference

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

Chairs Keohokalole and DeCoite and Members of the Committees:

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

This bill requires a business that provides an online service, product, or feature likely to be accessed by children to comply with certain data privacy requirements, including completing a data protection impact assessment, disclosing said assessment to the Attorney General pursuant to request, and prohibiting taking certain proscribed actions. This bill authorizes the Attorney General to seek an injunction or civil penalty against any business that violates certain provisions of this bill. This bill also creates the Hawaiʻi Children's Data Protection Working Group and requires reports to the Legislature.

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 the working group in section 2 of this bill.

Thank you for the opportunity to offer comments.

TESTIMONY OF TINA YAMAKI, PRESIDENT
RETAIL MERCHANTS OF HAWAII
FEBRUARY 13, 2024
SB 2012 RELATING TO ONLINE PRIVACY FOR CHILDREN.

Good morning, Chair Senator Keohokalole and Chair DeCoite and members of the Senate Committee on Commerce and Consumer Protection and the Senate Committee on Energy, Economic Development & Tourism 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 2012. This measure requires a business that provides an online service, product, or feature likely to be accessed by children to comply with certain data privacy requirements. Requires a business to complete a data protection impact assessment for any online service, product, or feature likely to be accessed by children and maintain documentation of the assessment as long as the online service, product, or feature is likely to be accessed by children; requires a business to make a data protection impact assessment available to the Attorney General pursuant to a written request and exempts a data protection impact assessment from public disclosure; prohibits a business that provides an online service, product, or feature likely to be accessed by children from taking certain proscribed actions; authorizes the Attorney General to seek an injunction or civil penalty against any business that violates certain provisions; creates the Hawai‘i Children's Data Protection Working Group; and requires reports to the Legislature.

Retailers like many businesses that have an online presence support protecting minors. However, it is our understanding that this bill as currently written takes after the California measure that was struck down by a Federal Judge on the grounds that the law's commercial speech restrictions violate the U.S. Constitution's First Amendment.

The Federal Government is currently putting together nationwide legislation that addresses children’s privacy on the internet. We should wait to see what the Federal Government’s restrictions are.

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

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 12, 2024

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

Senator Lynn DeCoite
Chair, Committee on Energy, Economic Development, and Tourism
Hawai'i State Capitol, Room 230
Honolulu, HI

RE: SB 2012 (Chang) – Age-Appropriate Design Code

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

On behalf of TechNet's member companies, I respectfully submit this letter of opposition to SB 2012, 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 2012 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 2012 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 2012 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 2012. 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

TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

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 2012.

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

February 13, 2024

Senator Jarrett Keohokalole, Chair
Senator Carol Fukunaga, Vice Chair
Senator Lynn DeCoite, Chair
Senator Glenn Wakai, Vice Chair

Re: In support of the ONLINE PRIVACY PROTECTION FOR CHILDREN (SB 2012)

Dear Chair members Keohokalole, Fukunaga, DeCoite, & Wakai,

For over 25 years, I served founders and venture capitalists as a trusted financial and investment advisor. In developing those confided relationships, I mentored senior executives, sitting alongside them, guiding product design, business strategy, and often personal leadership choices. These experiences provided insights into how companies create great client, customer, and user-focused products and services. Leading businesses excel in addressing their customers' existing problems and anticipating future needs, guiding them through a collaborative journey toward effective solutions with open and transparent communication. These businesses prioritize understanding and fulfilling the Best Interests of the Customer.

This background is critical because the provides a beneficial framework for businesses to conceptualize building Artificially Intelligent, Algorithmic, and Autonomous (AAA) based online products and services that help, rather than harm, consumers. SB 2012 Online Privacy Protection for Children (OPPC) will not only protect consumers, i.e. children, but guide companies in creating human-centric innovations that focus on solving customer problems. I will expand on this potential later.

With the proper perspective, businesses will see SB 2012 enabling ethical AI-based design that creates value for both companies and users and, and through that very relationship, for the State of Hawaii. It creates a how-to roadmap and provides the criteria every business should when innovating. This is essential for the largest global technology businesses to the start-up in their garage.

During my tenure as a Fellow at ForHumanity, a non-profit civil society organization dedicated to addressing risks associated with Ethics, Bias, Privacy, Trust, and Cybersecurity in Artificial Intelligence, Algorithmic, and Autonomous (AAA) Systems, I serve a critical role as a member of the Priority Drafting Team. Our primary task involves drafting AI audit certification schemes for various international laws, including Europe's General Data Protection Regulation, (GDPR), GDPR Children's Code, the EU AI Act, the Digital Services Act, the California Consumer Protection Act, and California's AADC. Our aim is to ensure a harmonized set of criteria, enabling compliance with one law to equate to compliance with all.

Our approach entails translating legal principles into business language, facilitating practical implementation. The certification scheme outlines a binary set of criteria (compliant/non-compliant), forming the basis for independent third-party audits of AAA Systems. Through these experiences, I offer my testimony in full support of SB 2012 Online Privacy Protection for Children.

My company, Holistic Ethics, LLC, and its flagship product, KidsTechEthics, stem from a comprehensive understanding of Children's Codes. We promote AI-based innovation in technology, making safer online spaces and digital experiences for children a reality. By incorporating ethical choices and Age-Appropriate Design principles, we create significant stakeholder value and a competitive advantage for early adopters. It is through this process of understanding of what a foundational child-centric Data Protection Impact Assessment should include, that we can recommend strategies and the remedies to mitigate risks.

OPPC aligns with evolving consumer expectations. It champions the design of products and services aligned with ethical standards, transparency, and accountability. This will enhance user trust, and foster a digital ecosystem where all stakeholders, including children, are valued and safeguarded. Contrary to what you may hear, this bill is pro-business, as it lays out the how to do it, and what to do for development and creation of ethical and responsible technologies. It guides business in considerations of they intend to use children's data and deliver them legal and appropriate content, services, and features.

This represents a significant opportunity to steer innovation in a positive direction, mitigating harms through demonstrated risk management frameworks, beneficial for both business and users. Embracing this code positions Hawaii as a pioneer in ethical technology practices, offering an attractive proposition for businesses valuing consumer protection and entrepreneurial growth.

It's crucial to address challenges raised by entities like NetChoice, which conflated children's privacy, product liability, with that of free speech. Section 230 protects platforms from user-generated content but doesn't absolve businesses from their duty of care and accountability for distribution of illegal content. SB 2012 focuses on the design methodology that platforms and businesses utilize in designing systems that deliver content, collect data, and influence users, particularly children, through AI, algorithms, and autonomous systems. Many businesses overlook understanding how their systems interact with users. This is a critical flaw you can correct.

While BigTech opposition raises few solutions and advocates for self-regulation, they fail to address harms caused by their algorithms, as evidenced by various legal actions. Documented evidence in the Attorney Generals v. Meta, which include Hawaii's Attorney General Anne Lopez, should stifle the arguments made by NetChoice and technology funded lobbyists that their products are safe, or that they have things under control. It is clear that investments made by many of the largest social media and technology businesses, including Meta, are the wrong ones. They are chasing shadows versus leading. This highlights the need for frameworks like SB 2012 to address ethical dimensions in content delivery, user interactions, and what will lead safety efforts as opposed to playing catchup.

SB 2012 wouldn't be necessary if social media and technology business placed consumer protections in their design frameworks from the start. For those seeking to innovate, OPPC will give them the framework to get it right. For those that choose not to take those precautions and/ or create the systems to mitigate know harms, this will provide a structure of accountability. Hawaii has a beautiful culture and set of traditions centered on ohana, this law ensures Hawaiian keiki are afforded protections when engaging in the digital world.

In conclusion, SB 2012 does not limit lawful speech to children. It is a product design and liability framework that protects how children's personal data is collected, processed, and considered in delivery of legal content. It strikes a balance between protecting children and fostering innovation. While refinements may be necessary, protecting vulnerable populations should remain paramount as technology advances.

Sincerely,

Jeffrey Kluge

Jeffrey Kluge
CEO & Founder Holistic Ethics, LLC, and Creator of KidsTechEthics
408-256-3757

February 13, 2024

LATE

Senate Committee on Commerce and Consumer Protection
Senate Committee on Energy, Economic Development, and Tourism
415 South Beretania Street
Honolulu, HI 96813

RE: SB 2012 - "RELATING TO ONLINE PRIVACY FOR CHILDREN." (Oppose)

Dear Chairs Keohokalole and DeCoite and Members of the Senate Committees on Commerce and Consumer Protection and on Energy, Economic Development, and Tourism:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SB 2012 in advance of the Joint Committees hearing on February 13, 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.

[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 disfavors. 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 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.

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 to a "reasonable level of certainty". CCIA suggests clarifying how businesses are expected to estimate the age of users online. Without a 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 2012 — if online services were to rely on self-attestation for estimates but

[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.
[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.

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 legislation may halt services for individuals under 18, hindering teenagers' internet access and, consequently, restricting their First Amendment right to information. This includes access to supportive online communities that might not be available 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 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

[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.
[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.

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 and Arkansas 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 both laws on hold until these challenges can be fully reviewed.[14] The fate of similar laws in Utah and Ohio 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 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

[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).
[15] *NetChoice, LLC v. Yost* (S.D. Ohio 2:24-cv-00047); *NetChoice, LLC v. Reyes* (D. Utah 2:23-cv-00911); *Zoulek et al. v. Hass & Reyes* (D. Utah 2:24-cv-00031).
[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.

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.

* * * * *

While we share the concerns of the sponsor and the Joint 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 Joint 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

[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/.

SB-2012
Submitted on: 2/9/2024 11:29:06 AM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
Katelyn Hirata	Individual	Support	In Person

Comments:

Senators,

My name is Katelyn and I'm 15 years old. I would like to voice my support for senate bill 2012. This bill should be passed because online safety is really important, especially for kids like us. We spend so much time online every single day for things like school, friends, or social media. When we're online, we share a lot of information about ourselves and we might not realize the impact it has. In the wrong hands, this information could be used to show us things we might not want to or be ready to see. It also can be really scary for us because it's constantly tracking you and what you do, your interests, and what you interact with. It's kind of like someone leaning over your shoulder watching everything you do. By protecting our data, it could add a layer of protection so that we can safely be online.

Thank you

SB-2012
Submitted on: 2/9/2024 1:17:34 PM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
Avery Higuchi	Individual	Support	In Person

Comments:

Good morning committee members of the CPN and EEP,

My name is Avery. I am a student at Mid-Pacific and we are learning about how our government works. I am writing to express my strong support for SB 2012, which aims to enhance data privacy protections for children accessing online services, products, or features in Hawaii. As a teenager, I understand the critical importance of safeguarding our youth's personal information in the digital age.

This bill represents a significant step forward in addressing the unique privacy challenges faced by children online. By requiring businesses to comply with specific data privacy requirements, this legislation prioritizes the well-being and safety of our youngest digital citizens. Even teenagers my age have trouble understanding if the website we are using is safe. It is so scary to realize that my profile is being sold to companies around the world of my interests and online activities, at the age of just 16. It's like bits of your personality and the most private parts of yourself are being sold online. It would bring many of us peace of mind, especially our parents, that we are being raised in a safe, yet informative world.

I urge you to support SB 2012. By enacting these crucial protections, we can create a safer online environment for our children and empower parents and guardians with the confidence that their children's personal data is being handled responsibly.

Thank you for considering my testimony in support of this vital legislation.

Sincerely,

Avery Higuchi

SB-2012
Submitted on: 2/11/2024 2:25:12 PM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
John Kailoa Pang	Individual	Support	In Person

Comments:

Hello, my name is Kailoa Pang, and I am a student at Mid-Pacific Institute. My classmates and I are following the legislature this year to better understand how our government works. I am writing this testimony to show my support for Senate Bill 2012.

This bill is a crucial part of today's world. My little brother is always online, and I want to ensure his data and privacy are kept safe. This bill can help make that happen. It requires companies offering online services for kids to do special checks to ensure they're not harming kids' privacy. These checks help them identify and fix any problems, such as showing kids inappropriate content or collecting too much personal information.

The bill also ensures that companies make it easy for kids and their parents to understand how their information is used and prevent them from tricking kids into sharing too much information. Additionally, there's a group of people who will monitor things and come up with even better ways to keep kids safe online.

By supporting this bill, we can ensure that not only us but also all future kids can enjoy the internet without worries.

Thank you for your time.

Kailoa Pang

SB-2012
Submitted on: 2/11/2024 10:28:25 PM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
Maya Wong	Individual	Support	In Person

Comments:

Good morning, committee members of the Committee on Consumer Protection and Commerce (CPN) and the Committee on Energy and Environmental Protection (EEP).

My name is Maya Wong, I am a high school student attending Mid-Pacific Institute. I stand before you today to express my support for SB2012, the Online Privacy Protection for Children Act. As a teenager navigating the digital society, I understand the importance of safeguarding our privacy online.

SB2012 is crucial for protecting students like me, from potential risks and threats on the internet. By requiring businesses to conduct data protection impact assessments and implement clear privacy settings, the bill encourages young users to navigate online platforms safely and securely.

As a high school student our lives are constantly intertwined with social media and various services for education, socialization, and entertainment. Our digital footprint is rapidly growing every day, and it is essential that we have measures in place to protect this information. SB2012 ensures that our personal information, including browsing habits, preferences, and communication data, remains protected from exploitation or misuse by online entities.

I commend the efforts to establish the Hawaii Children's Data Protection Working Group. This group will play a crucial role in developing better practices for implementing SB2012 and ensuring its effectiveness.

In conclusion, SB2012 is a vital step towards creating a safer digital environment for children and young adults like me. I urge you to support this important legislation for the well-being of our generation.

Thank you for your attention and consideration.

SB-2012
Submitted on: 2/12/2024 7:34:19 AM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
Ryan Kearns	Individual	Support	In Person

Comments:

Hello Senators,

My name is Ryan Kearns, I am a student of Mid Pacific Institute and a part of the MPX program.

I am here to express my strong support for Senate Bill 2012, as I believe that businesses should protect the privacy of minors. Minors have a right to privacy, and their data should not be sold or exploited in any way. I am concerned about the potential harm that could arise if this sensitive information falls into the wrong hands. I beg of you to pass this bill to help ensure the safety and well-being of the youth.

Thank you for your time and consideration.

SB-2012
Submitted on: 2/11/2024 10:30:55 PM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
Keanu Latu	Individual	Support	In Person

Comments:

Hello, my name is Keanu Latu and I am a 10th-grade student here to express my strong support for the Hawaii Children's Online Privacy Protection Act. This bill is crucial for safeguarding the privacy and well-being of students like myself in today's digital world.

The bill ensures that businesses must prioritize children's privacy by assessing and addressing potential risks associated with online services. It also establishes a working group to develop best practices for protecting children's online privacy rights.

As a student, I believe this bill is essential for creating a safe online environment and promoting responsible digital citizenship. Thank you for considering my perspective on this important issue.

Thank you for your time.

SB-2012
Submitted on: 2/12/2024 7:36:56 AM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
Luke Takakuwa-Holtey	Individual	Support	In Person

Comments:

Good Morning members of the CPN and EEP,

My name is Luke Takakuwa-Holtey, and I am a student at Mid-Pacific. I am reaching out to express my strong support for SB 2012, which aims to enhance digital privacy protections for minors using online services.

Growing up in the digital age, I have witnessed firsthand the importance of safeguarding our personal information online. The rapid advancements in technology have made it increasingly crucial to protect minors from potential threats and exploitation in the digital realm. SB 2012 presents a crucial step towards achieving this goal by holding businesses accountable for complying with data privacy regulations when handling minors' information.

As a teenager, I may not fully grasp the extent of the digital footprint left behind when sharing personal information online. However, the thought of my data being traded and sold without my consent is deeply concerning. It is even more alarming to consider the vulnerabilities faced by younger children whose private information may be exploited for nefarious purposes.

By supporting SB 2012, we can create a safer digital environment for minors and provide much-needed peace of mind for both children and parents. I urge you to consider the importance of this bill and its potential to address the pressing issue of digital privacy for our younger generation.

Thank you for your time and attention to this matter. Please give careful consideration to my testimony in support of SB 2012.

Sincerely,

Luke Takakuwa-Holtey

SB-2012
Submitted on: 2/12/2024 8:01:08 PM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
Buddy Hepton	Individual	Support	In Person

Comments:

Hi My name is Buddy Hepton with Mid-Pacific Institute, and I am in support with this bill.

SB-2012
Submitted on: 2/9/2024 7:41:41 AM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
Noah Chi	Individual	Support	Written Testimony Only

Comments:

Senators,

I am writing to express my support for Senate Bill No. 2012, which focuses on enhancing online privacy protections for children in our state. As an avid online 16 year old sophomore student, I understand the importance of safeguarding our personal information online.

This bill requires businesses to conduct assessments to identify and mitigate risks associated with online services for children. Additionally, it establishes a working group to develop best practices for children's online privacy.

I urge you to support Senate Bill No. 2012 to ensure the safety and privacy of children online.

Thank you for your attention to this matter.

SB-2012
Submitted on: 2/12/2024 8:04:58 AM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
Connor Yee	Individual	Support	Written Testimony Only

Comments:

Dear Senators,

I strongly support the Department of the Attorney General's measures outlined in the report on "Online Privacy Protection for Children." The requirement for businesses to conduct data protection impact assessments, with access granted to the Attorney General while maintaining privacy, is admirable. Prohibiting certain actions and empowering enforcement adds teeth to these safeguards. I support these efforts for a safer digital environment for Hawai‘i's children.

SB-2012
Submitted on: 2/12/2024 8:11:05 AM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
Xufeng	Individual	Support	Written Testimony Only

Comments:

Dear Senators

I am strongly in support of the Department of the Attorney General’s measures in the report regarding “Online privacy protection for children.”

The establishment of the Hawai‘i Children's Data Protection Working Group shows a commitment to finding solutions to protect children's online privacy. It's crucial that we prioritize children's safety online by implementing these recommendations.

Thank you for your attention.

Sincerely,

Xufeng

SB-2012
Submitted on: 2/12/2024 8:37:25 AM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
Raiden	Individual	Support	Written Testimony Only

Comments:

Good morning, committee members of Commerce and Consumer Protection and committee members of Energy and Environmental Protection.

I am Raiden Etscheit, a high school student at Mid-Pacific Institute. I am here today to testify in support of Senate Bill 2012, which focuses on online privacy protection for children in Hawai‘i.

As a young person who spends time online, I understand the importance of protecting our personal information, especially for children, who may be more vulnerable to potential risks. Senate Bill 2012 addresses this concern by introducing measures to protect children's online privacy rights.

The bill establishes clear definitions and guidelines for businesses that provide online services, products, or features likely to be accessed by children. It requires these businesses to conduct data protection impact assessments to identify and mitigate risks associated with their data management practices.

Furthermore, the bill prohibits businesses from engaging in certain practices, such as using personal information in ways that are detrimental to their physical or mental well-being or collecting unnecessary data without consent.

I believe that Senate Bill 2012 is a crucial step towards ensuring the safety and privacy of young internet users in our state. By implementing these measures, we can create a safer online environment where children can explore and learn without fear of exploitation or harm.

Thank you for considering my testimony, and I urge you to support Senate Bill 2012 for the benefit of all children in Hawai‘i.

Sincerely,
Raiden Etscheit

SB-2012
Submitted on: 2/12/2024 8:52:30 AM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
Alina	Individual	Support	Written Testimony Only

Comments:

Hi, I'm Alina, a student from Mid-Pacific, and I'm going to testify for Senate Bill 2012 relating to online privacy for children. Online privacy is crucial, especially for teens and young children, considering the evolving world and the continuous growth of the internet. Ensuring the safety of my generation and future ones is important.

As a teen using the internet daily, I want assurance that my data is secure and not susceptible to theft or sale. Despite being cautious online, it doesn't guarantee full protection from online dangers. If you have a child, you'd likely want to ensure their safety online, especially for young children who may not know better.

Emphasizing online safety is essential, and I appreciate your consideration of these matters. Thank you for reading.

SB-2012
Submitted on: 2/12/2024 8:59:46 AM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
Leilani	Individual	Support	Written Testimony Only

Comments:

Aloha, my name is Leilani Moran Hurtt. I am a student at Mid-Pacific and I am here to testify that I am in saport of the the bill SB 2012.

LATE

SB-2012
Submitted on: 2/12/2024 9:10:48 AM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
Shea	Individual	Support	Written Testimony Only

Comments:

Dear Legislators,

I am writing to express my strong support for the proposed bill regarding online privacy protection for children. As a student attending Mid-Pacific Institute in Hawaii, I am acutely aware of the significant role that the internet plays in our lives. While the digital world offers numerous opportunities for learning and connection, it also presents risks, especially for young people like myself.

This bill is crucial for safeguarding the online privacy and safety of children in Hawaii. It establishes essential protections and requirements for businesses offering online services, products, or features that are likely to be accessed by children. By mandating data protection impact assessments, the bill ensures that businesses thoroughly evaluate and address potential risks to children's privacy before offering their services.

As someone who frequently uses online platforms for educational purposes, socializing, and entertainment, I understand the importance of having clear privacy settings and protections in place. Being unaware of our digital vulnerability makes it difficult to trust any and all online platforms. By the time we're 18, who knows how much information they'll have already gathered. This could potentially affect not only our online experience but our physical safety too. How easy it already is to find an adults zip code, address, and telephone number. Can you even imagine how much simpler it'd be to trick an innocent naive child to willingly give up this information? All of this for just a few monetary transactions. Having my information sold online without my consent is absolutely unacceptable and I will not stand for it.

By enacting this bill, you will not only protect the privacy of children but also promote a culture of responsibility and accountability among businesses operating in the digital space. I urge you to support this bill to create a safer and more secure online environment for children in Hawaii.

Thank you for considering this bill and prioritizing the well-being of young people like me.

Sincerely,

Shea Yuen

Mid-Pacific Institute Student

LATE

SB-2012
Submitted on: 2/12/2024 9:20:15 AM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
Brennan Flores	Individual	Support	Written Testimony Only

Comments:

Hello everyone,

As a high school student who spends a lot of time online, I want to talk about why SB 2012 is so important to me. Everyone relies on the internet for everything such as entertainment, social media, education, and much more. But with that comes risks, especially when it comes to our privacy.

SB 2012 is all about making sure that the websites and apps we use are looking out for us. It requires them to do "data protection impact assessments," which means they have to think about how their sites might affect us and our personal information. They also have to set privacy settings to keep our information safe by default, which is awesome.

As a student athlete, I'm constantly getting scam text messages that appeal to me. For example, I get fake messages from college recruiters from a resource I've never used nor seen. Since I signed up for a different app for college recruiting, my information was sold to these scammers. This affects not only my safety, but my families. If people can just give away my phone number and details, what can they not get?

Plus, the bill stops companies from doing some really shady stuff, like using our information in ways that could hurt us or tracking us without us knowing. It's all about making sure we're safe and protected online.

I think SB 2012 is a no-brainer and very necessary for the protection of minors. We deserve to have our privacy respected and our online experiences kept safe. So, please support this bill and make sure it becomes a law. Our digital lives depend on it!

Thank you for listening.

LATE

SB-2012
Submitted on: 2/12/2024 11:53:59 AM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
phoenix carzino	Individual	Support	Written Testimony Only

Comments:

I am writing to express my strong support for bill SB2012, relating to online privacy for children, which establishes vital data privacy protections for children accessing online services in Hawaii. As a concerned citizen, I believe safeguarding children's personal information online is crucial.

The bill mandates businesses to conduct data protection assessments, prohibits certain actions, and enables enforcement by the Attorney General. The establishment of the Hawai‘i Children's Data Protection Working Group ensures ongoing oversight.

Please pass bill SB2012, relating to online privacy for children, to protect Hawai‘i's children online.

Sincerely,

Phoenix

SB-2012
Submitted on: 2/12/2024 8:41:37 PM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
Julian	Individual	Support	Written Testimony Only

Comments:

Aloha,

I'm Julian Romine, a student and Midpac and I support bill 2012.

Supporting a bill on online child privacy is imperative in safeguarding the digital well-being of our youngest users. Such legislation would establish stringent measures to protect children's personal information from exploitation by online platforms, ensuring their safety and privacy. By advocating for this bill, we prioritize the protection of vulnerable individuals in the digital landscape, fostering a safer online environment conducive to healthy development and growth. But I also think we should do this for ages 15 and under.

LATE

LATE

February 13, 2024

Senate Committee on Commerce and Consumer Protection
Senate Committee on Energy, Economic Development, and Tourism
415 South Beretania Street
Honolulu, HI 96813

RE: SB 2012 - "RELATING TO ONLINE PRIVACY FOR CHILDREN." (Oppose)

Dear Chairs Keohokalole and DeCoite and Members of the Senate Committees on Commerce and Consumer Protection and on Energy, Economic Development, and Tourism:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SB 2012 in advance of the Joint Committees hearing on February 13, 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.

[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 disfavors. 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 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.

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 to a "reasonable level of certainty". CCIA suggests clarifying how businesses are expected to estimate the age of users online. Without a 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 2012 — if online services were to rely on self-attestation for estimates but

[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.
[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.

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 legislation may halt services for individuals under 18, hindering teenagers' internet access and, consequently, restricting their First Amendment right to information. This includes access to supportive online communities that might not be available 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 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

[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.
[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.

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 and Arkansas 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 both laws on hold until these challenges can be fully reviewed.[14] The fate of similar laws in Utah and Ohio 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 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

[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).
[15] *NetChoice, LLC v. Yost* (S.D. Ohio 2:24-cv-00047); *NetChoice, LLC v. Reyes* (D. Utah 2:23-cv-00911); *Zoulek et al. v. Hass & Reyes* (D. Utah 2:24-cv-00031).
[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.

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.

* * * * *

While we share the concerns of the sponsor and the Joint 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 Joint 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

[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/.

LATE

LATE

SB-2012
Submitted on: 2/13/2024 1:45:20 PM
Testimony for CPN on 2/13/2024 9:00:00 AM

Submitted By	Organization	Testifier Position	Testify
Alex	Individual	Support	Written Testimony Only

Comments:

I support this bill.