JOSH GREEN, M.D.
GOVERNOR | KE KIA'ĀINA

SYLVIA LUKE
LIEUTENANT GOVERNOR | KA HOPE KIA'ĀINA

STATE OF HAWAII | KA MOKUʻĀINA ʻO HAWAIʻI
OFFICE OF THE DIRECTOR
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS
KA ʻOIHANA PILI KĀLEPA
335 MERCHANT STREET, ROOM 310
P.O. BOX 541
HONOLULU, HAWAII 96809
Phone Number: 1-844-808-DCCA (3222)
Fax Number: (808) 586-2856
cca.hawaii.gov

NADINE Y. ANDO
DIRECTOR | KA LUNA HOʻOKELE

DEAN I. HAZAMA
DEPUTY DIRECTOR | KA HOPE LUNA HOʻOKELE

Testimony of the Department of Commerce and Consumer Affairs

Before the
House Committee on Consumer Protection and Commerce
Tuesday, March 24, 2026
2:00 P.M.
Via Videoconference
Conference Room 329
On the following measure:
S.B. 2761, H.D. 1, RELATING TO SOCIAL MEDIA

Chair Matayoshi, and Members of the Committee:

My name is Radji Tolentino, and I am an Enforcement Attorney at the Department of Commerce and Consumer Affairs' (Department) Office of Consumer Protection (OCP). The Department offers comments.

The purposes of this measure are to require a social media platform to take reasonable steps to verify the age of new and existing account holders on the social media platform, prohibit a social media platform from allowing individuals under sixteen years of age from creating or maintaining an account or profile, absent the express consent from a parent or legal guardian and makes violations an unfair or deceptive act or practice in the conduct of trade or commerce.

We share the Legislature's concern about the harm caused by social media companies that use curation algorithms. Many social media platforms employ curation algorithms to maximize user engagement and may offer addictive, slot-machine-like features designed to keep children online longer because increased screen time drives

profit. These coercive design practices place children at risk even more so than adults, and voluntary industry action has failed to assuage concerns about harms to minors associated with prolonged social media use.

At the same time, we recognize that regulating social media access for minors presents significant legal and practical challenges. Several states, including Utah and Arkansas, enacted similar laws in 2023 that were subsequently blocked or challenged in court. Those efforts raised constitutional questions related to free speech and highlighted enforcement difficulties, particularly around age verification and the risk of infringing on user privacy. Utah has since enacted a different law requiring age verification at the app store level. No state that we are aware of has enacted a ban on minors under the age of sixteen creating an account on a social media platform.

Thank you for the opportunity to testify on this bill.

Amy Bos
Vice President of Government Affairs, NetChoice
1401 K Street NW, Ste 502
Washington, DC 20005

NetChoice
Defending Free Speech and Free Enterprise Online

Hawaii SB 2761

TESTIMONY IN OPPOSITION

March 24, 2026

Hawaii State Legislature

Committee on Consumer Protection and Commerce

Dear Chair Matayoshi, Vice-Chair Grandinetti, and Members of the Committee:

NetChoice respectfully submits this testimony in opposition to Hawaii SB 2761 HD1, which would require social media platforms to verify the age of all account holders and prohibit individuals under sixteen years of age from maintaining accounts without the express consent of a parent or legal guardian. NetChoice is a trade association of leading internet businesses that promotes the value, convenience, and choice that internet business models provide to American consumers. Our mission is to make the internet safe for free enterprise and free expression. As amended, SB 2761 HD1 raises significant concerns:

1. SB 2761 still raises First Amendment concerns and
2. SB 2761 would put Hawaii residents' privacy and data at risk, leaving them vulnerable to breaches and crime.

We share the sponsor's goal to better protect minors from harmful content online, but an unconstitutional law helps no one. NetChoice members have taken issues of teen safety seriously and in recent years have rolled out numerous new features, settings, parental tools, and protections to better empower parents and assist in monitoring their children's use of social media. We ask that you oppose SB 2761 and instead use this bill to jumpstart a larger conversation about how best to protect minors online by constitutionally sound legislation.

SB 2761 Violates the First Amendment

While the amended bill is a significant improvement over a blanket ban, it still imposes substantial burdens on the speech rights of minors. Social media platforms are forums for protected speech, and minors—including those under sixteen—have First Amendment rights that are well-established in Supreme Court precedent. In *Brown v. Entertainment Merchants Association*, the Court affirmed that "minors are entitled to a significant measure of First Amendment protection," and government efforts to restrict their access to constitutionally protected speech face strict scrutiny.[1]

[1] *Brown v. Entertainment Merchants' Ass'n*, 564 U.S. 786, 799 (2011) (invalidating California's attempt to ban minors from accessing "violent" video games because violent video games are protected speech)

While the amended bill is a significant improvement over a blanket ban, it still imposes substantial burdens on the speech rights of minors that may not survive constitutional scrutiny. Social media platforms are forums for protected speech, and minors—including those under sixteen—retain First Amendment rights recognized by the Supreme Court. The consent requirement, however well-intentioned, functions as a government-imposed prior restraint on a minor's ability to access constitutionally protected speech and association. Courts have generally been skeptical of licensing schemes that condition access to speech on advance government-approved gatekeeping, even when the gatekeeper is a parent rather than the state itself. The legislature should ensure that any consent mechanism is carefully structured to withstand that scrutiny, rather than risk having the entire framework invalidated.

Age Verification Requirements Create Serious Privacy and Security Risks

The bill's requirement that platforms take "reasonable steps" to verify the age of all users—new and existing—raises significant privacy concerns for every Hawaii resident who uses social media, not just minors. Meaningful age verification would necessarily require platforms to collect sensitive personal information such as government-issued IDs, biometric data, or financial information from all users.

This creates a massive honeypot of sensitive personal data vulnerable to breaches, hacking, and misuse. It also enables unprecedented surveillance and tracking of individuals' online activities. Users who value their privacy—including victims of domestic violence, political dissidents, or simply privacy-conscious individuals—would be forced to surrender identifying information as the price of accessing platforms for speech and association.

The bill does not define what "reasonable steps" means in practice, leaving platforms with significant legal uncertainty and potentially incentivizing them to adopt the most invasive verification methods to insulate themselves from liability. The legislature should consider providing clearer guidance that minimizes data collection while still achieving its child-protection goals.

An Approach that Actually Works

Rather than enact clearly unconstitutional laws banning the free speech of Hawaii residents, the state would be better served enacting laws that help the citizens and are legal. NetChoice is working with lawmakers from across the country to achieve such ends.

Requiring Digital Education in Schools

Empowering students with digital literacy skills and knowledge about online safety through curriculum developed by education experts represents a constitutional and effective approach. Such requirements effectively address crucial issues facing young people online. This approach will not only reach children where they are, but will help arm them to become better digital citizens.

Updating Child Abuse Laws for AI

Today, child abusers are able to use artificial intelligence to create images and escape justice under exiting Child Sexual Abuse Material (CSAM) laws. This is because existing CSAM laws require real images of the abuse, rather than AI generated ones. NetChoice is working with lawmakers to create laws that fill the gaps in existing CSAM laws to protect children from such abuses.

Empowering law enforcement to arrest child abusers

Today less than 1% of all reports of child abuse are even investigated. That means that 99% of reports of child abuse go unheard. This is because law enforcement doesn't have the resources it needs to investigate and prosecute child abusers. NetChoice supports giving law enforcement the resources it needs to put child abusers behind bars.

Again, we respectfully **ask you to oppose SB 2761** As always, we offer ourselves as a resource to discuss any of these issues with you in further detail, and we appreciate the opportunity to provide the committee with our thoughts on this important matter.[2]

Sincerely,

Amy Bos
Vice President of Government Affairs, NetChoice
NetChoice is a trade association that works to protect free expression and promote free enterprise online.

[2] The views of NetChoice expressed here do not necessarily represent the views of NetChoice members.

TECHNET
THE VOICE OF AMERICAN INNOVATION

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

March 22, 2026

Representative Scot Z. Matayoshi
Chair, Committee on Consumer Protection & Commerce
Hawaii State Capitol
415 South Beretania Street, Room 329
Honolulu, HI 96813

RE: SB 2761_SD2 HD1 (Keohokalole) – Relating to Social Media - Oppose

Dear Chair Matayoshi, and members of the committees,

On behalf of TechNet, we respectfully oppose SB 2761 SD2 HD1, which would prohibit social media platforms from providing accounts to individuals under the age of sixteen and impose affirmative obligations on platforms to prevent access by minors.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of American innovation by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes 100 dynamic American businesses ranging from startups to the most iconic companies on the planet and represents five million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

We share the Legislature's concern for youth mental health and support thoughtful, evidence-based approaches to protecting young people online. However, as drafted, SB 2761 SD2 HD1 would impose unworkable obligations, undermine privacy, and expose platforms to expansive liability without delivering clear or measurable benefits for minors.

<u>Knowledge Standard and Broad Access Ban</u>
While the Legislature's findings discuss concerns about algorithmic design and youth mental health, the operative provisions of SB 2761 SD2 HD1 do not regulate specific design features. Instead, the bill imposes a categorical prohibition on social media platforms from allowing individuals under sixteen to create or maintain accounts if the platform "knows" the individual is under sixteen years of age

The bill combines a knowledge-based prohibition with an undefined obligation to take "reasonable steps" to prevent minors from accessing accounts. This creates uncertainty about what level of age verification or monitoring would be required for compliance.

As with similar proposals in other states, SB 2761 SD2 HD1 places platforms in an untenable position: either collect significantly more personal information from all users, thereby raising privacy and security risks, or face enforcement exposure for failing to prevent access. This approach undermines longstanding privacy principles by incentivizing over-collection of sensitive data in the name of child protection.

A broad access ban tied to undefined "reasonable steps" does not provide clear, prospective compliance guidance and risks creating litigation-driven policy rather than predictable rules that protect young users.

Restricted Access to Lawful Speech and UDAP-Style Enforcement
When combined with the bill's UDAP-style enforcement mechanism, this structure exposes platforms to substantial liability based on subjective determinations of knowledge and reasonableness.

Because the bill conditions liability on a platform's knowledge of a user's age, it creates strong incentives for platforms to err on the side of denial—restricting access to lawful speech and information for both minors and adults. This is particularly concerning given that social media platforms are increasingly used for education, civic engagement, creative expression, and access to support resources. Broadly preventing minors under 16 from accessing social media platforms risks cutting minors off from beneficial content and online communities without tailoring protections to specific harms or high-risk behaviors. And, importantly, the bill's prohibition on access for minors under 16 takes away the rights of parents to decide what is best for their teens online.

Furthermore, SB 2761 SD2 HD1 heightens these concerns by deeming violations to constitute unfair or deceptive acts or practices. This UDAP-style enforcement mechanism significantly lowers the threshold for liability and introduces substantial uncertainty around compliance.

When combined with ambiguous standards—such as what it means for a platform to "know" a user's age or to take "reasonable steps" to prevent access—UDAP enforcement risks turning routine operational judgments into enforcement actions. This structure invites inconsistent application, retroactive second-guessing, and litigation-driven policy rather than clear, prospective rules.

Unintended Consequences for Privacy and Safety
By incentivizing aggressive age verification and account restriction, SB 2761 SD2 HD1 could paradoxically make online environments less safe. Young people may migrate to less-regulated platforms, use shared or fake credentials, or seek out unmoderated spaces without safeguards. At the same time, platforms may have fewer tools to provide age-appropriate content, safety features, or reporting mechanisms if minors are pushed off mainstream services.

TECHNET
THE VOICE OF AMERICAN INNOVATION

Protecting young people online is a critical and shared priority. However, SB 2761 SD2 HD1 adopts a blunt and impractical access ban, imposes infeasible compliance obligations, and exposes platforms to expansive UDAP liability without clear standards.

We respectfully urge the Legislature to consider more targeted, evidence-based alternatives that focus on specific high-risk behaviors, strengthen parental and user controls, and preserve privacy while supporting youth well-being.

For these reasons, we respectfully oppose SB 2761 SD2 HD1.

If you have any questions regarding our position, please contact Robert Boykin at rboykin@technet.org or 408.898.7145.

Sincerely,

Robert Boykin
Executive Director for California and the Southwest
TechNet

March 24, 2026

House Committee on Health and House Committee on Human Services and Homelessness
Hawaii State Capitol
415 South Beretania St.
Honolulu, HI 96813

Re: SB 2761 – "Relating to Social Media" (Oppose)

Dear Chairs Marten, Chair Takayama, and Members of the Joint House Committee on Health and House Committee on Human Services and Homelessness:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SB 2761. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] Proposed regulations on the interstate provision of digital services therefore can have a significant impact on CCIA members.

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

However, protecting children from harm online does not include a generalized power to restrict ideas to which one may be exposed. Lawful speech cannot be suppressed solely to protect young online users from ideas or images that a legislative body disfavors.[4] As the bill's legislative findings now acknowledge, "minors also have a First Amendment right to free speech. A narrowly-tailored approach that protects minors from the harms proposed by social media, while still enabling minors to engage in constitutionally protected speech, is therefore needed." While CCIA shares the goal of increasing online safety, this bill presents the following concerns.

---

[1] For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

[2] Competitive Enterprise Institute, *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/ (last updated June 10, 2025).

[3] Jordan Rodell, *Why Implementing Education is a Logical Starting Point for Children's Safety Online*, Disruptive Competition Project (Feb. 7, 2023), https://project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/.

[4] *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 212–14 (1975). *See also FCC v. Pacifica Found.* 438 U.S. 726, 749–50 (1978); *Pinkus v. United States*, 436 U.S. 293, 296–98 (1978).

U.S. courts have repeatedly struck down laws containing speech restrictions intended to prevent harm to minors.

In 1997, the Supreme Court held that "the First Amendment does not tolerate" laws that "reduce[] the adult population ... to reading only what is fit for children."[5] Yet SB 2761 effectively does exactly this: in order to restrict access to content potentially harmful to children, the proposed bill would restrict both children and adults' access to such content. The First Amendment applies to teens as well as adults,[6] and includes their right to speak anonymously online.[7]

Nor do states have the authority to require parental consent for viewing such content; the Court has likewise rejected the argument that "the state has the power to prevent children from hearing or saying anything without their parents' prior consent."[8] Accordingly, the proposed bills unconstitutionally undermine established free speech protections for users of all ages. As the bill's legislative findings now recognize, the First Amendment applies to teens as well as adults,[9] and includes their right to speak anonymously online.[10]

For these reasons, the vast majority of lower courts that have ruled on the issue have held that the First Amendment does not permit states to require age verification to access protected speech.[11] As a Louisiana federal court recently held when striking down a similar law, "The Act's age-verification and parental-consent requirements fail strict and intermediate scrutiny. Even if the Court accepts that Defendants have a compelling interest 'in protecting the physical and psychological well-being of minors,' Defendants have not established a causal relationship between social media use and health harms to minors."[12]

SB 2761's method of designating covered services violates the First and Fourteenth Amendments.

The bill's coverage definition also poses constitutional problems: SB 2761 covers online services and applications based in part on whether they "primarily serve[] as a medium for users to interact with content generated by other users". Multiple federal courts have found this method of designating covered services to violate the First Amendment's prohibition on content-based speech restrictions and/or the Fourteenth Amendment's prohibition on vague laws.[13] As it is impossible to objectively determine which of an online service's purposes or

[5] *Reno v. ACLU*, 521 U.S. 844, 888 (1997) (cleaned up).
[6] *See, e.g.*, *id.* at 855-56.
[7] *See, e.g.*, *NetChoice v. Griffin*, No. 23-cv-05105, 2025 WL 978607 at *20-21 ((W.D. Ark. Mar. 31, 2025).
[8] *Brown v. Ent. Merchs. Ass'n*, 564 U.S. 786, 795 n. 3 (2011).
[9] *See, e.g.*, *id.* at 855-56.
[10] *See, e.g.*, *Griffin*, 2025 WL 978607 at *20-21.
[11] *See, e.g.*, *NetChoice v. Jones*, No. 1:25-cv-02067 (E.D. Va. Feb. 27, 2026); *CCIA v. Paxton*, No. 25-cv-01660, 2025 WL 3754045 (W.D. Tex. Dec. 23, 2025); *SEAT v. Paxton*, No. 25-cv-01662, 2025 WL 3731733 (W.D. Tex. Dec. 23, 2025); *NetChoice v. Murrill*, No. 25-231, 2025 WL 3634112 (M.D. La. Dec. 15, 2025); *NetChoice v. Carr*, 789 F. Supp. 3d 1200 (N.D. Ga. 2025); *NetChoice v. Yost*, 778 F. Supp. 3d 923 (S.D. Ohio 2025); *Griffin*, 2025 WL 978607; *NetChoice v. Reyes*, 748 F. Supp. 3d 1105 (D. Utah 2024); *CCIA v. Paxton*, 747 F. Supp. 3d 1011 (W.D. Tex. 2024).
[12] *Murrill*, 2025 WL 3634112 at *72 (cleaned up).
[13] *See, e.g.*, *Jones*, No. 1:25-cv-02067 at *16-19; *Murrill*, 2025 WL 3634112 at *86-88; *Yost*, 778 F. Supp. 3d at 952-58; *Griffin*, 2025 WL 978607 at *34-40; *SEAT*, 765 F. Supp. 3d at 594; *CCIA*, 747 F. Supp. 3d at 1032-24.

functions is its "primary" one, such services will not know whether the law applies to them. As an Arkansas federal court recently explained when invalidating a similarly worded statute, the law's framing "does not define… a term critical to determining which entities fall within its scope,"[14] thereby "leaving companies to guess whether their online services are covered."[15]

The above phrasing further violates the First Amendment by regulating speech based on a digital service's content. As a Virginia federal court recently explained, "creat[ing] an exemption for content preselected by the provider and not generated by users… favors provider-selected speech over user generated speech…. precisely the type of speaker preference the Supreme Court declared should be treated as content-based."[16] Several other federal courts have found such content-based regulation of digital service to be unconstitutional as well.[17]

Age verification and parental consent requirements undermine user privacy for users of all ages.

SB 2761 contains many requirements that undermine privacy for all users. While well-meaning, age verification mandates inherently require collecting sensitive data about users and adults. Such policies run contrary to the data minimization principles underlying federal and international best practices for privacy protection.[18] Requiring individuals to share sensitive personal information with third parties, including IDs or biometrics, can make recipients a prime target for identity theft, cyberattacks, or other data breaches.[19] Such dangers are far from hypothetical: several of the most devastating data breaches in recent years are directly attributable to age verification requirements.[20] Furthermore, government officials could access this sensitive data through enforcement inquiries and processes.

The more data a service is forced to collect, the greater risk it poses to consumer privacy and small business sustainability.[21] A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, found that "smaller companies may not be able to sustain their business" if forced to implement costly age verification methods, and that

[14] *Griffin*, 2025 WL 978607 at *36.
[15] *Id.* at *37.
[16] *Jones*, No. 1:25-cv-02067 at *18 (cleaned up) (quoting *Reed v. Town of Gilbert, AZ*, 576 U.S. 155, 170 (2015)).
[17] *See, e.g.*, *Murrill*, 2025 WL 3634112 at *62; *Yost*, 778 F. Supp. 3d at 953; *Griffin*, 2025 WL 978607 at *22-24.
[18] *See, e.g.*, *Fair Information Practice Principles (FIPPs)*, Fed. Privacy Council, https://www.fpc.gov/resources/fipps/; *Principle (c): Data Minimisation,* U.K. Info. Comm'r Off., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/.
[19] Shoshana Weissmann, *Age-Verification Legislation Discourages Data Minimization, Even When Legislators Don't Intend That*, R St. Inst. (May 24, 2023), https://www.rstreet.org/commentary/age-verification-legislation-discourages-data-minimization-even-when-legislators-dont-intend-that/.
[20] *See, e.g.*, Mark Tsagas, *Online Age Checking Is Creating a Treasure Trove of Data for Hackers*, The Conversation (Nov. 11, 2025), https://theconversation.com/online-age-checking-is-creating-a-treasure-trove-of-data-for-hackers-268586.
[21] Engine, *More Than Just a Number: How Determining User Age Impacts Startups* (Aug. 2024), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/66ad1ff867b7114cc6f16b00/1722621944736/More+Than+Just+A+Number+-+Updated+August+2024.pdf.

"[h]ighly accurate age assurance methods may depend on collection of new personal data such as facial imagery or government-issued ID."[22]

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.[23] Though the intention to keep kids safe online is commendable, this bill undermines that initiative by requiring more data collection about young people.

Restricting access to the internet for younger users limits their access to information and supportive communities.

Requiring businesses to deny access to social networking sites or other online resources may also unintentionally restrict children's ability to access and connect with like-minded individuals and communities. For example, since children of certain minority groups may not live in areas where they can easily connect with others who relate to their unique experiences, an online meeting place to share such experiences and find support can have positive impacts.[24]

Empirical findings regarding social media's impact on young users are much more nuanced than SB 2761's introductory legislative findings suggest. When the U.S. Surgeon General released the advisory entitled *Social Media and Youth Mental Health* referenced in these findings, many were quick to highlight only the harms and risks it detailed, as did the original version of this bill. However, as the legislative findings now acknowledge, the advisory is much more complex and also discusses many potential benefits of social media use among children and adolescents. It concludes, for instance, that social media provides young people with communities and connections with others who share identities, abilities, and interests.[25] It can also provide access to important information and create spaces for self-expression. Research further details that social media can especially benefit marginalized youth, including racial, ethnic, sexual, and gender minorities, as online peer support can mitigate the stresses they face.[26]Indeed, as an Ohio court noted when striking down a law age-gating social media services last year, "nearly all of the research showing any harmful effects" for minors on social media "is based on correlation, not evidence of causation."[27]

---

[22] *Age Assurance: Guiding Principles and Best Practices*, Digital Trust & Safety Partnership (Sept. 2023) at 10, https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.
[23] *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.
[24] *The Importance of Belonging: Developmental Context of Adolescence*, Boston Children's Hospital Digital Wellness Lab (Oct. 2024), https://digitalwellnesslab.org/research-briefs/young-peoples-sense-of-belonging-online/.
[25] Off. of the Surgeon Gen., U.S. Department of Health & Human Services, *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory*, *Social Media Has Both Positive and Negative Impacts on Children and Adolescents* (2023), https://www.ncbi.nlm.nih.gov/books/NBK594763/.
[26] *Id.*; *see also* Jennifer Marino et al., *Social Media Use and Health and Well-being of Lesbian, Gay, Bisexual, Transgender, and Queer Youth: Systematic Review*, J. Med. Internet Rsch. (Sept. 22, 2021), https://www.jmir.org/2022/9/e38449.
[27] *NetChoice v. Yost*, 778 F. Supp. 3d 923, 955 (S.D. Ohio 2025).

As explained above, CCIA believes that an alternative to solving these complex issues is to work with businesses to continue their ongoing private efforts to implement mechanisms such as daily time limits or child-safe searching so that parents can have control over their own child's social media use.

To avoid restricting teens' access to information, SB 2761 should regulate users under 13 rather than 16 in accordance with established practices.

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 15-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 would suggest changing the scope of covered users to be minors under the age of 13 to align with the federal Children's Online Privacy Protection Act (COPPA) standard.[28] 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.

* * * * *

We appreciate the Committee's consideration of these comments and stand ready to provide additional information as the Legislature considers proposals related to technology policy.

Sincerely,

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

[28] *See* 15 U.S.C. § 6501(1).

KOBAYASHI SUGITA & GODA, LLP
Attorneys at Law

Bert T. Kobayashi, Jr.*
Alan M. Goda*
Charles W. Gall*
Neal T. Gota
Charles D. Hunter
Robert K. Ichikawa*
Christopher T. Kobayashi*
Jan M. L. Y. Kutsunai*
David M. Louie*
Nicholas R. Monlux
Aaron R. Mun
Bruce A. Nakamura*
Kenneth M. Nakasone*
Harry Y. Oda
Jesse W. Schiel*
Craig K. Shikuma*
Timothy T. Silvester
Lex R. Smith*
Joseph A. Stewart*
Brian D. Tongg
David B. Tongg*
Caycie K. G. Wong
*A Law Corporation

Of Counsel:
Kenneth Y. Sugita*
John R. Aube*
Wendell H. Fuji*
Clifford K. Higa*
Burt T. Lau*
Larry L. Myers*
Gregory M. Sato*
David Y. Suzuki*
Andrew M. Carmody
Ashley L. Choo
Olivia D. Grodzka
Ying Gu
Justin Hart
Drew K. Ichikawa
Daniel K. Jacob
Austin H. Jim On
Stephen G. K. Kaneshiro
Travis Y. Kuwahara
Ryan D. Louie
Zachary K. Shikada
Reece Y. Tanaka

March 23, 2026

COMMITTEE ON CONSUMER PROTECTION & COMMERCE
Rep. Scot Z. Matayoshi, Chair
Rep. Tina Nakada Grandinetti, Vice Chair

HEARING DATE: March 24, 2026
TIME: 2:00 p.m.
PLACE: Conference Room 329

Re: TESTIMONY ON BEHALF OF META OPPOSING SENATE BILL 2761, SD2, HD 1

Dear Chair Matayoshi, Vice Chair Grandinetti, and Members of the Consumer Protection & Commerce Committee:

Thank you for the opportunity to testify today. My name is David Louie, and I am here on behalf of Meta. We share the legislature's goal of ensuring safe, positive online experiences for young people. We appreciate that this bill has moved away from a blanket under-16 social media ban and toward a framework focused on age assurance and parental consent. That shift is a constructive step because it better reflects the central role parents play in guiding their teens' online lives and the benefits that social media may bring to teens, including building community and exploring interests.

However, we must oppose the bill as written. Requiring age verification and parental consent on an app-by-app basis is not workable for families, would lead to inconsistent protections across the broader app ecosystem, and raises significant privacy and data security concerns.

An app-by-app mandate would require parents to repeat the same steps across the many apps their teens use. Research shows that teens use roughly 40 apps per week, and that could translate into a different verification and consent process for each app. That level of repetition is unrealistic for busy families and risks reducing meaningful oversight. The more fragmented and burdensome the process becomes, the harder it is for parents to stay consistently engaged.

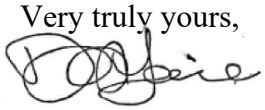
The app-by-app approach also increases privacy and security risks by distributing sensitive information across many more entities. Rather than minimizing the collection and handling of sensitive data, an app-by-app system multiplies the number of apps and vendors that may be asked to collect, process, or store information like IDs, birth certificates, or other personal data. Families should not have to provide sensitive information repeatedly across a wide range of services when the same policy goal can be achieved through a more centralized and privacy-protective approach. In addition, compliance costs will be significant: larger companies may be able to build complex verification systems, but smaller or emerging services often cannot, creating further divergence of safety outcomes. We believe there is a better way to achieve the same goal of putting parents in charge of the apps their teens want to use.

Meta believes the most effective, consistent, and privacy-protective approach is to place age assurance and parental approval at the app store or operating system level, at the point of download. Busy parents should be able to give permission in one place before a teen downloads an app. This approach is more realistic for families, creates consistent standards across the ecosystem, and reduces duplication. It can also be designed so apps receive only a limited eligibility signal, such as an age range or confirmation that parental approval has been provided, rather than receiving identity documents or other sensitive data. That reduces collection, limits exposure, and better protects families' privacy.

Though we believe age verification and parental consent should occur at the App Store level, we want to be clear that Meta is still investing heavily in teen safety. In recent years, we rolled out Teen Accounts for Instagram, Facebook, and Messenger—our fundamentally reimagined experience that gives parents peace of mind and helps keep teens safe online. With Teen Accounts, teens are automatically defaulted into protective settings limiting who can contact them, the content they see, and making sure their time is well spent. Any teen under 16 will need a parent to make these settings less strict. And we continue to build on these protections. Most recently, we revamped our content policies on Instagram so that content teens see is inspired by movie ratings for ages 13+ by default. This means teens under 18 are automatically placed into a 13+ content setting and will see content similar to what they'd see in an age-appropriate movie. We've also introduced a stricter "Limited Content" setting for parents who prefer more restrictive content experiences for their teens. We will continue improving these protections, and we agree legislation can play a constructive role, especially when it focuses on scalable solutions that work across the broader ecosystem.

We appreciate the direction of the bill's recent amendments, but we remain concerned that an app-by-app framework will be confusing for parents, inconsistent in practice, and riskier for privacy and security. For these reasons, we respectfully oppose the bill as written and urge the Committee to consider an app store or OS-level approach that empowers parents, protects privacy, applies more uniformly, and delivers consistent protections for teens across the ecosystem. Please find language for the App Store model attached to this testimony below. We look forward to partnering with you to help keep kids safe online.

Very truly yours,



DAVID M. LOUIE
for
KOBAYASHI SUGITA & GODA, LLP

Enclosure: Exhibit A

EXHIBIT “A”

S./H.R. ____

A BILL

To empower parents to exercise supervision over their children's online experiences.

SECTION 1. SHORT TITLE.

This Act may be cited as the "Parental Empowerment Act".

SEC. 2. FINDINGS.

The legislature finds the following:

(1) internet-ready devices, and the applications that run on such devices, are used by millions of individuals under the age of 16 on a daily basis;

(2) more than 75% of parents believe teens under 16 should not be able to download apps without parental permission, according to a poll conducted by Morning Consult in November 2023;

(3) operating systems today already know the stated age of users, the apps they use, have parental permission and approval built into the download step under certain circumstances, and are already using such a parental approval system for their own purchases as confirmed in public statements in other regulatory proceedings such as Apple's white paper "Complying with the Digital Markets Act, Apple's Efforts to Protect User Security and Privacy in the European Union," March 2024, *available at* https://developer.apple.com/security/complying-with-the-dma.pdf;

(4) so-called "app stores" offer the most efficient, efficacious and privacy protective setting to empower parents to institute their choices over children's internet usage; and

(5) there is a compelling governmental interest in empowering parents to protect their children online and doing so through parental consent and age assurance requirements is narrowly tailored to further that interest.

SEC. 3. Definitions.

(a) In this section:

(1) APPLICATION.—The term “application” means a software application or electronic service that may be run or directed by a user on a computer, a mobile device, or any other general purpose computing device.

(2) APPLICATION STORE.—The term “application store” means a publicly available website, software application, electronic service, or platform that distributes and facilitates the download of applications from third-party developers to users of a computer, a mobile device, or any other general purpose computing device.

(4) CHILD.-- The term “child” means an individual under 16 years of age.

(5) COMMISSION.—The term “commission” means the Federal Trade Commission.

(6) COVERED COMPANY.—The term “covered company” means any person, entity, or organization that owns, controls, or operates an application store or operating system that serves customers in [STATE].

(7) DEVELOPER.—The term “developer” means any person, entity or organization that creates, owns, or controls a public-facing website, online service, online application, or mobile application.

(8) OPERATING SYSTEM.— Any entity that develops, maintains, or distributes an operating system on a computer, mobile device, or any other general purpose computing device.

SEC. 4 EMPOWERING PARENTS TO PROTECT THEIR CHILDREN.

(a) Covered Company Obligations.—A covered company shall:

- **(i)** Take commercially reasonable steps to determine or estimate age:
  - **(1)** For new users, at account creation; and
  - **(2)** For existing users, within six months of the effective date of this act.
- **(ii)** Obtain parental or guardian consent prior to:
  - **(1)** Permitting a child to download an application distributed or made accessible via the covered company’s application store, if the covered company provides an application store; or
  - **(2)** Permitting a child to access an application pre-loaded or side-loaded onto a device for the first time, if the the covered company provides an operating system;

(iii) If the covered company provides an application store, provide an API or other mechanism that allows the developer of an app in the provider's app store that is downloaded by a minor to connect with the approving parent for the sole purpose of facilitating the approving parent's use of the developer's parental controls, including the features outlined in Sec.4(b); and

(iv) Provide all developers, including developers of pre-loaded or side-loaded applications, upon request with a signal via a real-time application programming interface on an ongoing basis regarding whether parental or guardian consent has been provided, if applicable, and whether an individual is:

(1) Under the age of thirteen,
(2) At least thirteen years of age and under sixteen years of age,
(3) At least sixteen years of age and under eighteen years of age; or
(4) At least eighteen years of age;

(b) Developer Obligations.—A developer shall:

(i) Request an age and parental consent signal for each individual from an applicable covered company upon account creation or first access and may request additional age signals thereafter.

(ii) Use such signal from a covered company to:

(1) Enforce legally required minimum age restrictions,
(2) Ensure compliance with all laws and other obligations, and
(3) Provide any age appropriate defaults, safeguards or experiences, except as provided in this section.

(iii) To the extent applicable and technically feasible, provide readily available features for a parent or guardian to oversee a child's use of the application as appropriate to the risks that arise from the child's use of the developer's application. The features provided shall include:

i. **Time Restrictions.** The ability to view metrics reflecting the amount of time that the child is using the application and set daily time limits on the child's use;
ii. **Social Connection Information.** The ability to see which individuals or accounts are affirmatively linked to the child, such as the child's friends, followers, or accounts that the child is following;
iii. **Profile Visibility.** The ability to determine whether the child has limited the public visibility of their profile or information and content uploaded to the application;
iv. **Block Lists.** The ability to see which individuals the child has blocked; and,

v. **Reporting.** The ability to submit a report to the application concerning a potential violation of its terms and policies.

(c) Signal Reconciliation.—

(i) If a developer determines that an internal age signal conflicts with the age signal from a Covered Company, the developer may rely on the signal from the Covered Company unless the developer has actual knowledge that an internal signal is more accurate. If the developer has actual knowledge that its internal signal is more accurate, such as if the user provided proof of age to the developer, the developer shall use such internal signal.

(ii) To the extent applicable and technically feasible, a developer shall transmit the conflicting internal age signal back to a covered company via a mechanism provided by the covered company in instances where the developer has actual knowledge that an internal signal is more accurate.

(iii) Upon receipt of a conflicting internal age signal from a developer, the covered company shall take steps to re-verify the user's age and update the age signal accordingly to provide developers with the newly verified age

SEC. 5. ENFORCEMENT AND OTHER MATTERS.

(a) NO PRIVATE RIGHT OF ACTION; PRESERVATION OF CERTAIN IMMUNITY.— This subsection does not create a private right of action under this Chapter or any other law or diminish or adversely affect protections for a developer or covered company under section 230 of the Communications Act of 1934 (47 U.S.C. 230).

(b) ENFORCEMENT.

(i) Only a minor, or the parent of that minor, who has been harmed by a violation of Subsection 13-75-201(2) may bring a civil action against an app store provider.

(ii) Only a minor, or the parent of that minor, who has been harmed by a violation of Subsection 13-75-202(4) may bring a civil action against a developer.

(c) In an action described in Subsection (2), the court shall award a prevailing parent:

(i) The greater of:

(1) Actual damages; or

(2) $1,000 for each violation;

(3) Reasonable attorney fees; and

(4) Litigation costs.

(d) PROHIBITION ON ANTICOMPETITIVE CONDUCT.—

(1) Nothing in this Act, or any amendment made by this Act, shall be construed to modify, impair, or supersede the operation of any of the antitrust laws, unless otherwise specified.

(2) A covered company shall comply with this Act in a nondiscriminatory manner, specifically including, but not limited to:

(i) A covered company shall impose at least the same restrictions and obligations on its own applications and application distribution as it does on those from third party applications or application distributors.

(ii) A covered company shall not use data collected from third parties, or consent mechanisms deployed for third parties, in the course of compliance with this Act to compete against those third parties, give the covered company's services preference relative to those of third parties, or to otherwise use this data or consent mechanism in an anticompetitive manner.

(e) DEVELOPER SAFE HARBOR.—

(1) **Reliance on Signal.** A developer is not liable under applicable law if the developer relied on age signal or parental consent information provided to the developer by a covered company or, in instances where a developer has actual knowledge that an internal age signal is more accurate, relied on such internal signal.

(2) **Signal Reconciliation.** A developer shall not be liable for transmitting an internal age signal to a covered company for purposes of reconciling conflicting age signals.

Testimony in Opposition to SB2761_HD1

March 22, 2026

Part I: Greetings and Introduction

Dear chairpersons and members of the committee,

Thank you for reading my testimony. After the bill's most recent revision from the HSH hearing, SB2761_HD1 has become explicit age-verification (AV) mandate. The old provisions from the SD2 version of being required to enter one's birth date upon the creation of a social media account has been replaced with social media platforms needing to take "reasonable steps" to verify the ages of both new and existing users. The only "reasonable steps" to verify a user's age is through AV that involves the invasive scanning government photo IDs, personally-identifying financial documents, and biometric face scans of the user's face and then uploading it to an AV service and/or the social media platform itself. As a Hawaii resident who will have to live under this law, I strongly oppose SB2761_HD1.

Part II: SB2761_HD1 and Age-Verification (AV) Will Harm Artists, the LGBTQ+ Community, the Poor, the Disabled, People of Color, and Immigrants

I am an amateur artist who shares art online and is part of an online art community (assuming it shows up, I have included a relevant piece of artwork at the end). My freedom to express myself and to connect with my community is threatened by AV that SB2761_HD1 will impose. I rely on small niche art posting websites to share my art and to connect with my community which would be classified as social media as it allows user-generated content and is primarily for users to interact with such content; should SB2761_HD1 become law, I would be locked out from using those sites as these sites do not have the funds to implement AV. I am deathly afraid that my time as an artist maybe coming to an end because SB2761_HD1 will leave me with nowhere to showcase my work and no place to communicate with fellow artists. Online art communities are threatened by AV because it aims to restrict mature and provocative art which is an inherent part of art and these communities; bans and restriction on mature and provocative art by platforms that try to remain compliant with AV and other online safety laws usually degenerate into overreaching censorship of most art in general. Related to this, as AV and other online safety laws leads to the censorship of more and more art, financial institutions are taking notice and have begun to cut payment services for artists which is absolutely ruinous for the many artists who make a living off of their work.

As noted by digital rights group Electronic Frontier Foundation (EFF), there are many minority and vulnerable groups will be disenfranchised by AV[1]. Online art communities are home to some of these groups. Many artists are poor; the poor are disenfranchised by AV because they cannot afford to obtain and keep updated the ID documentation needed for AV. Many artists are from the LGBTQ+ community; AV disenfranchises them because it cuts them off from adult-friendly online communities that are one of the few places that openly welcome them, it restricts access for life-saving LGBTQ+ resources, and, especially for those who are transgender and non-binary, AV discriminates against them as it is difficult for them to get or update ID documents that accurately reflects their new gender and name. Many artists are disabled and art is their only option to make a living; AV discriminates against the disabled as those with facial differences cannot pass AV face scans, most are ineligible for a driver's

license, and it is very difficult for them to get other ID documents as, again, many are too poor to afford it and many are physically unable to get it as their disability makes it difficult to reach government offices that process ID applications.

Beyond the poor, the LGBTQ+ community, and the disabled, AV also disenfranchises people of color. As AV face scans are primarily designed to judge the ages of white people, adult people of color are disproportionately misidentified as minors and they are also disproportionately among the poor who cannot afford ID documents. This concern is especially troubling for Hawaii due to our incredibly diverse population; many Hawaii residents could end up shut out of much of the internet for simply not being white. Immigrants too are discriminated against by AV as many are ineligible for certain ID documents and, as many are also poor, cannot afford the ID they are eligible for. AV is anti-poor, anti-LGBTQ+, transphobic, ableist, racist, and xenophobic.

Part III: SB2761_HD1 and AV Will Harm the Kids and Teens They are Supposed to Protect

Then there are the kids and teens AV is supposed to protect. Soon after Australia imposed its social media ban for those under 16 via AV, there has been anecdotal reports of a significant increase in kids seeking mental health services.[2] In addition, disabled Australian teens either already have been or fear losing access to social media because the ban not only cuts them off from friends and support communities, the loss of social media is the loss of one the last bits of freedom afforded to them from their physical/mental limitations.[3] AV cuts off kids from their friends and communities as well as increasingly infringes on their already limited free speech rights. LGBTQ+ youths completely lose access to life-saving resources and support as there is an increasing push to condemn anything regarding the LGBTQ+ community as inherently "harmful to minors." Teens in general lose access to sexual health resources that not only can save their lives, it can also prevent lifelong mistakes. Homeschooling for kids could become next to impossible as AV could end up restricting their ability to do research, take online courses, and take remote exams. Students from any academic settings could be locked out of wealth of information important to their education from history and politics to literature and other media.

Something that has been missing in the political debate over AV and other online safety legislation that seeks to restrict minors' access to social media and other online services is the views and opinions of the kids who will actually be most affected by these laws. In 2024, the digital rights group Electronic Frontier Foundation (EFF) conducted a survey of thousands of young people between the ages of under 16 into their 20s about how social media benefited them and and how they would feel about losing accessing to social media in regards to the potential passage of the Kid's Online Safety Act (KOSA; a Congressional bill that, like SB2761, seeks to restrict minors' access to social media).[4] According to EFF's findings, teens feared losing their freedom of speech/expression and their right to privacy, losing their right to be accurately informed and understand the world around them, being cut off from friends and community, and being inhibited from their ability to even understand themselves. Many of the interviewees were from the LGBTQ+ community who stressed how social media is an important sanctuary for them as the outside world becomes increasingly hostile. In addition, in something that hits close to home for me as an amateur artist, many young artists fear that a restriction on social media would both impede their ability to develop their skills and take away valuable opportunities to do their passion as a living. I see myself in these young artists and I too fear the same things as an adult.

SB2761_HD1 did make some revisions to allow those under 16 to use social media if they have the explicit permission of their parents/guardian (I will collectively refer to both as “parents” from here on). While this did address some of the concerns over a blanket ban over social media for minors under 16, there are serious lingering problems as well as new ones caused by the insistence on AV in this most recent revision of the bill. First, the kids and teens in question still do not actually have their protected right to free speech; it still belongs to that of their parents as they still need to give them permission. This may not be much of an issue in many cases in which parents/guardians have the best interest of their children in mind; however, this is a dangerous problem for children whose parents do not have their best interest in mind like in cases of neglect or abuse; abusive and neglectful parents would be given an even greater ability to isolate their victims. Outside of such cases, even when parents would want to give permission for their children to use social media, they may still be deterred because of AV. AV would require the parents to scan and upload their IDs and faces and, therefore, put all of that personally-identifying data at risk of being leaked to the public in inevitable data breaches of AV services and be made vulnerable to the likes of identity theft and scams (I will discuss more about the privacy problems surrounding AV in the next part). Related to this, since SB2761_HD1’s restrictions applies to those under the age of 16, minors aged 16 and 17 will need to through AV themselves to use social media and be required to upload ID and face scans that, like parents, are put at risk of being leaked to the public and put them also in danger of identity theft and scams. Last, but definitely not least, there are the kids in the foster system; as they do not have parents or other legal guardians who could give explicit permission to use social media, they are unfairly locked out completely. SB2761_HD1’s “theoretical” respect for the free speech rights of kids and teens does not exist in reality. Instead, the free speech rights of both children and their parents are violated and both are made vulnerable from the dangerous invasions of privacy brought about by AV.

Part IV: SB2761_HD1’s AV Mandate Destroys Privacy, Puts People At Risk to Government Overreach, and Upends How the Internet Works

There are the already well-known privacy concerns surrounding AV which have been realized in the high-profile mass data breaches/leaks involving ID verification like that of the women’s dating safety app Tea (13,000 face scans exposed)[5], the chat service Discord (70,000 users had their IDs exposed)[6], and the ID verification service AU10TIX (ID scans and other personally identifying information were exposed from users of major online platforms such as TikTok, X, and Uber who hired AU10TIX to do ID verification)[7]. The largest data leak yet involving ID verification happened in late 2025 to the ID verification service IDMerit which leaked ID scans and other personally-identifying information of approximately 1 billion users worldwide, including over 200 million American users.[8] AV services and social media platforms cannot protect the sensitive private data they are required to collect. A new related concern emerging in the aftermath of the increasingly violent anti-immigration raids in states like Minnesota is that government agencies will force AV services to share the ID data they have collected in order to help facilitate those anti-immigration raids. This is becoming realized as Homeland Security demanded popular social media platforms and other internet services to reveal the true identities of accounts who criticized their anti-immigration actions.[9] AV service Persona, who performed verification for the likes of OpenAI, video game platform Roblox, and briefly for Discord, was caught mass surveilling and profiling its users which included comparing their ID data with government databases and watchlists.[10]

At the beginning of March, concerns over AV legislation being passed by governments all over the world led to an open letter by 438 researchers and scientists who specialize in digital privacy and

security from 32 countries that pointed out critical flaws of AV.[11] The official link to the letter can be found here: https://csa-scientist-open-letter.org/ageverif-Feb2026 . The letter includes the infeasibility of deploying AV effectively as seen in the explosion of ways to circumvent AV (which is caused by the need for many adults who cannot pass AV needing alternative ways to access information and services locked behind it), the failure of AI-based age estimation/assurance which is heavily error-prone, the disruptions caused by AV (like locking up important site features) making online services increasingly more difficult to use, and the underestimation by governments on the infrastructure needed to make AV work well and be secure in order for there to be mass adoption and acceptance by the public. Without that mass adoption and acceptance by the public, AV can never be effective.

The open letter also includes how there is a poor understanding by the governments implementing AV laws on what harms AV can bring such as both adults and minors migrating to fringe and potentially dangerous websites that neither complies with AV nor any other internet regulations, a false sense of security for parents/guardians (as AV can be circumvented and kids will likely migrate to those non-compliant websites), a dangerous diminishing of online privacy that is essential for the online safety of everyone and the fundamental functioning of the internet, discrimination against people who cannot pass AV (such as the various groups of people mentioned previously who cannot obtain ID documentation and/or cannot pass biometric face scans), and the dangerous centralization of power by those who get to decide what content should or should not be locked behind AV (a particular danger for LGBTQ+ people as acceptance and tolerance of them is in decline). Most grievous of all, the letter concludes that there is NO scientific evidence that AV protects minors from mental stress caused by social media use and, instead, may actually harm them by cutting them off from beneficial resources, services, and support which, in-turn, cannot justify AV mandates that threaten to bring about all of the previous harms and problems mentioned in the letter. The open letter by these experts generally reflects many of the points made here about the dangers of AV mandates and of SB2761_HD1.

Part V: SB2761_HD1 and AV is Unconstitutional

The various problems mentioned here about AV laws and serious questions about even their effectiveness in protecting minors have led to these laws becoming challenged in the courts and ultimately losing those legal battles. A case in point is NetChoice v. Murrill which saw Louisiana's Act 456, a social media AV law similar to SB2761_HD1, become permanently blocked in US District Court for the Middle District of Louisiana back in mid-December.[12] The most serious judgement is that AV laws violates free speech protections of the First Amendment; NetChoice compares the mandatory ID verification of AV laws used to restrict access to websites to having mandatory ID checks before entering a public library which is forbidden by the First Amendment. The courts are increasingly finding AV laws to be unconstitutional. SB2761_HD1's AV mandate is unconstitutional and violates the First Amendment because AV prevents many groups who cannot pass AV (such as the LGBTQ+ community, the poor, the disabled, people of color, immigrants, and kids/teens) from accessing social media to exercise their free speech rights and, even for those who can pass AV, the serious privacy concerns over AV will deter many of them too. The very fact that SB2761 could be found to be unconstitutional in the courts is even noted by the testimonies of the Department of the Attorney General and the Department of Commerce and Consumer Affairs. I am disappointed and dismayed that the Department of the Attorney General, despite knowing this, not only keeps pushing for the passage of SB2761, but also wrote the revisions for SB2761_HD1 that has transformed the bill into an overexpansive AV mandate that will affect all social media users in Hawaii, the same kind of law that

was and struck down in NetChoice v. Murrill for being in violation of the very legal foundations of the US.

Part VI: SB2761_HD1 and AV Could Inhibit State Government Functions

As government functions increasingly relies on social media, I believe there are some relevant concerns for committee members, the rest of the state legislature, and the entire state government over AV and social media restrictions. First, many state representatives use social media for outreach to their constituency and send out important messages. If social media should be restricted by AV, would one's constituency be willing to upload their ID and/or go through a face scan to reach out to you on social media? If your constituency cannot easily reach you, will they still vote for you? As the ID and biometric requirements will likely lead to many Hawaii users fleeing major social media platforms, it may become much harder for elected officials to gauge the political sentiments their own constituencies and push out relevant messaging; that could lead to more unpredictable and expensive electoral races as candidates have to commit much more time and money in a struggle to understand their own voters.

Another concern for government functions has to do with the emergency broadcast system. In recollecting over what happened during last summer's tsunami emergency and the largely successful evacuation, unrestricted social media played a critical life-saving role as official emergency messages were posted on and government press conferences were streamed through them. The reach of this critical messaging was significantly amplified by people on social media reposting those official government messages and press conferences. I myself was keeping up with the quickly developing news about the tsunami through Reddit and YouTube. The quick and far reaching dispersal of emergency messaging over social media played a role in helping a great many Hawaii residents and visitors heed the warnings in a timely manner and allowed for the largely successful evacuation. This has continued to be the case during the recent rainstorms and flooding. During those heavy storms which caused mass power outages, checking social media through cell service allowed members of my family to check in on their friends and co-workers as well as to see when power would be restored from Hawaiian Electric. At the time of me typing this, our own Governor Josh Green had posted important information regarding the storms like satellite tracking and emergency radio stations on his Facebook and Instagram social media pages; Facebook and Instagram both require users to have accounts to browse most the site in which new and current users would have to go through AV should SB2761_HD1 become law. Social media has allowed people to remain in close contact with each other and with vital government resources in dangerous times. Should social media become heavily restricted by AV, will emergency messaging be able to be reach Hawaii residents and visitors in a timely manner? Are people willing and able to upload ID and/or go through a face scan to see those messages? Should SB2761_HD1 lead to a mass migration of Hawaii users off of major social media platforms, combined with the declining use of other live media like television and radio, many Hawaii residents and visitors could become difficult to reach and left woefully uninformed during emergencies. This could be a case in which restricting social media may cost lives.

Part VII: Conclusion

I understand there is a powerful undercurrent right now going through governments across the US and around the world to punish Big Tech and reign in their excesses. However, bills and laws like SB2761_HD1, ironically, empower Big Tech more than ever. Should SB2761_HD1 become law, smaller websites are simply shut out of Hawaii completely while large social media platforms become

the only options left as they can afford AV and weather the inevitable lawsuits and fines. It is the normal everyday people of Hawaii who will be punished by AV. Everyone's free speech rights and right to privacy are violated, artists lose their livelihoods, and vulnerable minorities become locked out of much of the internet; kids and teens especially lose access to a number valuable and even life-saving and resources from friends to support communities to accurate information about anything while increasingly rogue federal agencies are given a powerful tool to target the people of Hawaii; many of you here may become disconnected your constituencies and stand to lose future elections and more people may die in future emergencies and natural disasters as urgent emergency messaging may not reach many Hawaii's residents and visitors in time. Again, I am urging you here to oppose SB2761_HD1. Thank you for your time, consideration, and hard work.

Sincerely,
Cary

1 The Electronic Frontier Foundation's (EFF) article about the dangers of AV, which includes many the various groups disenfranchised by AV: https://www.eff.org/deeplinks/2025/12/10-not-so-hidden-dangers-age-verification

2 A BlueSky post from University of New South Wales Professor Deborah Lupton, PhD MPH revealing an increase in Australian kids seeking mental health services after the implementation of the country's social media ban for minors: https://bsky.app/profile/dalupton.bsky.social/post/3mcv3gudi2s2h

3 The Guardian's article about the worries of disabled Australian teens in the aftermath of the social media ban: https://www.theguardian.com/australia-news/2026/feb/06/ive-lost-my-friends-advocacy-groups-warn-australias-social-media-ban-risks-isolating-kids-with-disabilities?CMP=Share_iOSApp_Other

4 The EFF's article about its survey of young people in regards to how social media has benefited them and their thoughts on the restriction of social media by legislation like the Kids' Online Safety Act (KOSA): https://www.eff.org/deeplinks/2024/03/thousands-young-people-told-us-why-kids-online-safety-act-will-be-harmful-minors

5 CNET's article about the Tea app data breach: https://www.cnet.com/tech/services-and-software/the-tea-app-data-breach-what-was-exposed-and-what-we-know-about-the-class-action-lawsuit/

6 Cyber Security News' article about the Discord data breach: https://cybersecuritynews.com/discord-data-breach-sensitive-data/

7 Gizmodo's article about the AU10TIX data leak: https://gizmodo.com/identity-verification-firm-used-by-x-tiktok-and-uber-1851562934

8 Cybernews' article about the IDMerit data leak: https://cybernews.com/security/global-data-leak-exposes-billion-records/

9 A New York Times article about Homeland Security subpoenaing social media platforms to reveal the identities of users who criticize their anti-immigration actions: https://www.nytimes.com/2026/02/13/technology/dhs-anti-ice-social-media.html?unlocked_article_code=1.MFA.84qB.K9Z-Z1EJdyGt

10 The Rage's article about AV service Persona's mass surveillance of its users: https://www.therage.co/persona-age-verification/

11 Cybernews' article about the open letter from an international group digital privacy and security researchers criticizing AV legislation: https://cybernews.com/privacy/scientists-slam-brakes-age-verification-laws-teens/

12 NetChoice's article about its legal victory in NetChoice v. Murrill: https://netchoice.org/netchoice-wins-permanent-block-of-louisiana-age-verification-law-protecting-free-speech-and-parental-rights/

SB-2761-HD-1
Submitted on: 3/23/2026 1:24:16 PM
Testimony for CPC on 3/24/2026 2:00:00 PM

Submitted By	Organization	Testifier Position	Testify
D. C.	Individual	Comments	Written Testimony Only

Comments:

To paraphrase George R. R. Martin, “The internet is dark and full of terrors.” While it is clear that social media platforms such as those maintained by Meta and xAI are quite harmful to mostly everyone and we all should stop using them for our collective mental health, there are much more squalid, darker, seedy corners of the internet.

While gatekeeping youth from the arguably toxic grip of Zuckerberg and Musk is an honorable endeavor no doubt, the unintended consequences suggest SB 2761 and its various reiterations would incentivize these youth to find alternatives. Dark alternatives that have little to no regulation or oversight. The legislature may be solving one problem but creating a vastly bigger one in the process. The legislature (and every sane human) would certainly prefer youth to be on Facebook or Instagram rather than on 4chan, which does not require an account to post.

It is also unclear how violations of chapter 480, HRS, would be prosecuted for out of state and foreign operations. Are unenforceable laws truly laws?

The house draft one is a slight improvement over the senate drafts, but the underlying problems remain.

It still seems the better solution would be to mandate a social media education course in the Department of Education about the dangers and proper usage of social media.

LATE

SB-2761-HD-1
Submitted on: 3/24/2026 12:19:19 PM
Testimony for CPC on 3/24/2026 2:00:00 PM

Submitted By	Organization	Testifier Position	Testify
Simon Matthew David	Individual	Oppose	Written Testimony Only

Comments:

Dear Chair and Committee Members,

I am writing to oppose Senate Bill 2761.

I understand the concerns that motivate this proposal. Many parents are worried about how social media affects young people, and protecting kids online is an important goal. However, a blanket ban on social media accounts for everyone under the age of 16 is an overly broad response.

In Hawai‘i, families are often spread across different islands or across the mainland. Because of that distance, many teenagers rely on social media to stay connected with relatives they do not see regularly. Messaging and sharing updates online allow them to remain part of everyday family life even when they are physically far apart. Removing access does not just reduce screen time — it can also cut off an important way young people maintain relationships with family members.

Rather than prohibiting access altogether, a more practical solution would be to give parents stronger tools to guide their children’s online activity. Requiring age verification and parental approval through app stores could provide a single, straightforward checkpoint for families while still allowing teens to communicate with the people who matter most to them.

For these reasons, I respectfully ask the committee to reject SB 2761 and consider alternatives that support both youth safety and family connection.

Thank you for your time and consideration.

SB-2761-HD-1
Submitted on: 3/24/2026 12:27:08 PM
Testimony for CPC on 3/24/2026 2:00:00 PM

LATE

Submitted By	Organization	Testifier Position	Testify
Leinaala Keohuhu-Paaluhi	Individual	Oppose	Written Testimony Only

Comments:

Dear Chair and Members of the Committee,

I respectfully ask you to vote no on Senate Bill 2761, which would bar youth under the age of 16 from having social media accounts. While I appreciate the concern driving this proposal and agree that online safety is an important issue, this bill takes an overly broad approach that may do more harm than good.

For many young people in Hawai‘i, social media is not simply entertainment. It is a primary way they maintain relationships with friends and family who live on neighbor islands or on the mainland. Teens use these platforms to stay in touch with grandparents, siblings, and cousins they may only see occasionally. Removing access may reduce screen time, but it also severs meaningful connections that help young people feel supported and engaged in their communities.

Additionally, the bill does not consistently address the areas of greatest concern. By exempting gaming and other online platforms, it leaves open spaces where documented risks to children already exist. Experiences in other countries show that broad prohibitions often drive youth toward less regulated or more anonymous corners of the internet, where oversight is weaker and risks may be higher.

Rather than an outright ban, a more effective solution would be to require age verification and parental approval at the app store level. This would provide parents with a centralized, practical tool to guide their children’s online access without cutting off communication entirely. Families differ in their values and circumstances, and parents should be empowered to make decisions that reflect those differences.

LATE

For these reasons, I urge you to oppose SB 2761 and pursue policies that strengthen parental involvement and genuinely enhance youth safety.

Thank you for your consideration.

SB-2761-HD-1
Submitted on: 3/24/2026 12:27:12 PM
Testimony for CPC on 3/24/2026 2:00:00 PM

LATE

Submitted By	Organization	Testifier Position	Testify
Eveni-Elijah Aipoalani-Tuaoi-Tootoo	Individual	Oppose	Written Testimony Only

Comments:

Aloha Chair and Committee Members,

I am writing in opposition to Senate Bill 2761. Although protecting young people online is a goal we all share, prohibiting anyone under 16 from using social media is not the right solution.

In Hawai‘i, distance is a reality for many families. Teens often rely on social media to maintain close relationships with relatives living on different islands or across the continent. These platforms allow them to participate in family life, share milestones, and maintain daily communication in ways that phone calls or occasional visits cannot fully replace. Eliminating access does not just reduce exposure to risk — it also limits connection, belonging, and community.

Furthermore, SB 2761 excludes certain online spaces, including gaming platforms, where safety concerns have already been documented. A partial ban that leaves these environments untouched may simply shift youth activity to platforms with fewer safeguards and less transparency. International examples have demonstrated that sweeping age bans rarely remove teens from the digital world; instead, they push activity underground, making supervision more difficult.

A more balanced approach would focus on giving parents clear authority and practical tools. Implementing age verification and parental consent requirements through app stores would create a single checkpoint for families while preserving the ability to stay connected. This respects parental responsibility and allows families to make decisions based on their own children’s maturity and needs.

LATE

I respectfully ask you to oppose SB 2761 and consider alternatives that prioritize both safety and family connection.

Mahalo for your time and service.

SB-2761-HD-1
Submitted on: 3/24/2026 12:28:20 PM
Testimony for CPC on 3/24/2026 2:00:00 PM

LATE

Submitted By	Organization	Testifier Position	Testify
Nalani-Tearsjah Aipoalani-Tuaoi-To'oto'o	Individual	Oppose	Written Testimony Only

Comments:

Aloha Members,

I am writing to urge you to oppose Senate Bill 2761, which would prohibit individuals under 16 from creating or maintaining social media accounts. I commend the legislature for addressing the issue of teen safety online, but unfortunately, this is the wrong approach.

For many teens, social media is how they stay connected with friends and family members on other islands or the mainland. It's also how they keep up with younger cousins they don't get to see every day. These are important relationships that social media helps young people maintain in ways that weren't possible before. Yess, cutting that off that access limits screen time, but more pressingly, it cuts teenagers off from their families and communities.

The bill also doesn't target the right platforms. SB 2761 carves out gaming platforms and other services, meaning places like Roblox (where child predators have been documented targeting young users) are completely untouched. We've seen in Australia that sweeping bans like this don't get kids off the internet. They push them toward less regulated, harder-to-monitor platforms. That makes kids less safe.

There is a better approach. Requiring age verification and parental consent at the app store level would give parents a single, streamlined point of control without cutting young people off from the connections they rely on. It empowers parents to make decisions for their own families rather than leaving that judgment entirely to the government.

I urge you to oppose SB 2761 and support solutions that actually work for Hawai'i's families.