TESTIMONY OF
THE DEPARTMENT OF THE ATTORNEY GENERAL
KA ʻOIHANA O KA LOIO KUHINA
THIRTY-THIRD LEGISLATURE, 2026

ON THE FOLLOWING MEASURE:
S.B. NO. 2761, S.D. 2, H.D. 2, RELATING TO SOCIAL MEDIA.

BEFORE THE:
HOUSE COMMITTEE ON JUDICIARY & HAWAIIAN AFFAIRS

DATE: Wednesday, April 1, 2026 **TIME:** 2:00 p.m.

LOCATION: State Capitol, Room 325

TESTIFIER(S): Anne E. Lopez, Attorney General, or
Ashley M. Tanaka, Deputy Attorney General

Chair Tarnas and Members of the Committee:

The Department of the Attorney General (Department) provides the following comments.

Section 2 of this bill adds to part I of chapter 481B, Hawaii Revised Statutes (HRS), a new section to require digital application store providers to verify the age of users, require parental consent for users under sixteen years of age to download or purchase, or make a purchase on, a social media platform, and distribute that information to social media platforms. It also requires social media platforms to obtain the age information from digital application store providers, determine whether parental consent has been provided for young persons, and take reasonable steps to identify young person users through their algorithms.

This bill may present a greater risk of First Amendment litigation than prior versions of the bill. In addition to prohibiting individuals under the age of sixteen from downloading or purchasing a social media platform or making purchases on a social media platform (page 5, lines 11-13), this bill also requires age verification for all new digital application store account holders before they can download and access any application store content. Page 5, lines 1-7. Although restricting minors' access to social media platforms without parental consent raises similar First Amendment implications whether the age verification and parental consent process occurs at the application store or application level, this bill restricts access to a broader range of

speech because it requires all application store users, including adults, to verify their age regardless of which apps they wish to download. A district court in Texas preliminarily enjoined a similar law as violating the First Amendment because it would be "akin to a law that would require every bookstore to verify the age of every customer at the door." Computer & Communications Indus. Ass'n v. Paxton, No. 1:25-CV-1660-RP, 2025 WL 3754045, at *1 (W.D. Tex. Dec. 23, 2025).

Thank you for the opportunity to testify.

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 Judiciary and Hawaiian Affairs
Wednesday, April 1, 2026
2:00 P.M.
Via Videoconference
Conference Room 325
On the following measure:
S.B. 2761, H.D. 2, RELATING TO SOCIAL MEDIA

Chair Tarnas 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 requires a digital application store provider to verify the age of users, require parental consent for users under sixteen years of age to download or purchase, or make a purchase on, a social media platform, distribute that information to social media platforms, require social media platforms to obtain the age information from digital application store providers, determine whether parental consent has been provided for young persons, and take reasonable steps to identify young person users through their algorithms.

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 laws in 2023 to regulate minors' access to social media that were subsequently blocked or challenged in court. These efforts raised constitutional concerns related to free speech and highlighted enforcement difficulties, particularly around age verification and risks to user privacy. Utah has since enacted a law similar to this measure, requiring age verification at the app store level, which has also faced legal challenges.

The measure's age verification provisions raise important considerations for how consumer data is handled. In other states, age verification laws typically include limited safeguards—such as collecting only what is necessary, restricting use of the data, and requiring deletion after verification—while broader data protections are addressed through separate comprehensive privacy laws. This measure does not clearly define these limits, which may lead to unnecessary data collection and increased risk of misuse or breaches. Clear guardrails on data collection, use, and retention would help better protect consumers while supporting effective implementation. For example, states like Louisiana and Texas require that personal data collected for age verification be used only for that purpose and deleted after verification is complete, reflecting a data minimization approach.

Thank you for the opportunity to testify on this bill.

Amy Bos
Vice President Government Affairs, NetChoice
Washington, DC 20005

NetChoice
Protecting Free Speech and Free Enterprise Online

Hawaii SB 2761, App Store Bill

TESTIMONY IN OPPOSITION

March 31, 2026

Hawaii Legislature
House Committee on Judiciary and Hawaiian Affairs

Dear Chair Tarnas, Vice-Chair Poepoe and Members of the Judiciary and Hawaiian Affairs Committee,

NetChoice respectfully urges the committee to oppose SB 2761, which mirrors Texas Senate Bill 2420 — a law a federal court blocked in December 2025 as unconstitutional — and tracks similar legislation now facing a constitutional challenge in Utah. Like those laws, SB 2761 would require app stores to verify users' ages and obtain parental consent before minors can download or purchase applications.

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.

We share the sponsor's goal to better protect minors from harmful content online. NetChoice members have taken the issues of children's and teen safety seriously and, in recent years, have rolled out new features, settings, parental tools, and protections to better empower parents and help them monitor their children's use of social media. We ask that you oppose age verification proposals and instead focus on proposals that more effectively protect young people online without violating the constitutional rights of every Hawaiian of any age.

Age Verification–whether at the app store level, device or website-level raises constitutional issues—and is now being litigated in other states.

The Supreme Court and other federal courts have ruled that age verification mandates that block access to the exercise of First Amendment rights are unconstitutional. Age verification laws have recently failed to withstand legal scrutiny in California, Utah, Ohio, Arkansas, and Louisiana.[1] Implementing such a

[1] See NetChoice v. Reyes, D.Utah (2023), https://netchoice.org/netchoice-v-reyes/; NetChoice v. Yost, S.D.Ohio (2024), https://netchoice.org/netchoice-v-yost/.

measure in Hawaii would likely meet the same fate and lead to costly legal challenges without providing any real benefits to the state's residents. As Federal Judge Freeman noted in granting a full injunction against California age restriction law, "The act applies to *all* online content likely to be accessed by consumers under the age of 18, and imposes significant burdens on the providers of that content."[2]

In December 2025, U.S. District Judge Robert Pitman blocked Texas SB 2420, the App Store Accountability Act, from taking effect. The Computer & Communications Industry Association (CCIA) successfully challenged the law, which would have required app stores to verify users' ages and obtain parental consent for minors- provisions nearly identical to those in SB 2761. The court ruled that "SB 2420 is unconstitutional in the vast majority of its applications" under the First Amendment and compared the law to requiring every bookstore to verify the age of every customer at the door and demand parental consent before a child could enter or purchase a book.[3]

Given that legal landscape, SB 2761's age-verification, parental-consent requirements, and data-related requirements cannot survive judicial review. Unlike regulating access to physical products no one has a constitutionally enumerated right to buy (cigarettes, alcohol), requiring ID (or similar "identity-based" burdens) for accessing lawful speech violates the First Amendment rights of adults, minors, and businesses alike. "Age-verification schemes," a federal district court recently held in enjoining Arkansas's similar age-verification requirements, "are not only an additional hassle, but they also require that website visitors forgo the anonymity otherwise available on the internet."

Finally, SB 2761 would likely be ruled unconstitutional under the Dormant Commerce Clause because it regulates behavior and activities that take place outside of Hawaii. The law also imposes requirements on app stores about users who are under the age of 18. These requirements conflict with COPPA, a federal law that governs how websites handle minors' data. Therefore, SB 2761 also violates the Constitution's Supremacy Clause.

Age Verification proposals undermine parental authority.

Poorly-designed age verification laws not only face legal challenges, but also encroach upon parents' long-established prerogatives in guiding their children's upbringing and online activities. Many online

[2] NetChoice v. Bonta Case No. 22-cv-08861-BLF
[3] *Computer & Communications Industry Association v. Paxton*, Case No. 1:25-cv-01660-RP (W.D. Tex. Dec. 23, 2025)

platforms have already implemented robust parental control features. For example, some online platforms have led the way with suites of tools for parents and teens to better protect themselves. Additional parental controls are available at the device level. For example, iPhones and iPads already empower parents to limit the time their children can spend on the device, choose which applications (e.g., YouTube, Facebook, Snapchat, or Instagram) their children can use, set age-related content restrictions for those applications, filter online content, and control privacy settings. Market-driven innovation allows for diverse solutions that address different needs and preferences.

Moreover, if onerous requirements are forced onto app stores or devices, minors will quickly shift their access to use browsers instead of specialized apps, circumventing the protections the law aims to establish. This highlights the ineffectiveness of device-level or app store-level verification as a comprehensive solution.

Simply put, a one-size-fits-all government mandate will give users a false sense of security and will flatten the offerings for youth safety that are currently provided by the private sector. It would stifle innovation in this space and potentially reduce protections for Hawaiian youth, as companies focus on compliance rather than developing more effective, tailored solutions.

Age Verification proposals would put Hawaiians' private data at risk, leaving them vulnerable to breaches and crime.

From a privacy standpoint, implementing age verification could compromise user's sensitive data. Americans value their privacy and the ability to use online services without unnecessary intrusion. Age verification systems would require collecting and storing sensitive personal data, potentially including government-issued IDs or biometric information. This not only contradicts the bipartisan aim of improving data security but also creates a new target for cybercriminals, potentially putting Hawaiians at risk of identity theft or other forms of fraud. As we know from recent experience, any time there is a store of sensitive information it becomes a prime target for identity thieves and other nefarious individuals. Even government agencies have fallen victim to these attacks.

A quarter of minors become a victim of identity fraud or theft before their 18th birthday.[4] The problem is even worse for minors in foster care and child welfare systems. Identity fraud incidents can affect a

[4] 25 percent of kids will face identity theft before turning 18. Age-verification laws will make this worse. - R Street Institute (2024).

young person's credit reports, holding them back on the path to financial stability. Age verification mandates stand to make this problem a catastrophe.

Conclusion

While app store age-verification proposals are well-intended, NetChoice strongly believes that the drawbacks outweigh potential benefits. We respectfully urge the committee to reject this unconstitutional and ineffective approach. Instead, we encourage fostering private sector innovation in parental controls and youth safety tools. NetChoice members remain committed to protecting minors online through empowering parents, educating users, and working with policymakers to develop more effective and constitutional solutions to address concerns about underage access to sensitive content or services.

We want to be a resource to discuss these issues in further detail, and we appreciate the opportunity to provide the committee with our thoughts on this important matter.

Sincerely,

Amy Bos, Vice President Government Affairs, NetChoice[5]

NetChoice is a trade association that works to protect free expression and promote free enterprise online.

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

PRIDE AT WORK Hawai'i

Where the LGBTQIA+ equality & Labor movements meet!
A constituency group of the Hawai'i State AFL-CIO

March 31, 2026

House's Committee on Judiciary & Hawaiian Affairs
Hawai'i State Capitol
415 South Beretania Street
Honolulu, HI 96813

Hearing: Wednesday, April 1, 2026, at 2:00 PM

RE: **Opposition for Senate Bill 2671 SD 2 HD 2 - RELATING TO SOCIAL MEDIA**

Aloha Chair Tarnas, Vice Chair Poepoe, and fellow committee members,

Pride at Work – Hawai'i is an official chapter of *Pride at Work* which is a national nonprofit organization that represents LGBTQIA+ union members and their allies. We are an officially recognized constituency group of the AFL-CIO that organizes mutual support between the organized Labor Movement and the LGBTQIA+ Community to further social and economic justice.

Pride at Work – Hawai'i respectfully submits testimony in opposition to Senate Bill 2671.

We agree with the underlying concern that social media platforms must do more to protect users, especially our keiki, from harmful and false information. The rapid spread of misinformation and disinformation online has real-world consequences, and stronger accountability for these billion-dollar revenue generating platforms is both necessary and long overdue.

However, SB 2671 takes an approach that raises serious concerns about privacy, worker rights, and unintended harm to vulnerable communities, including māhū, LGBTQIA+, and QTPI+ young people.

Requiring digital application store providers to verify users' ages and distribute that data to social media companies creates a centralized system for collecting and sharing highly sensitive personal information. This presents significant risks, including data breaches, misuse of personal data, and increased surveillance of individuals' online activity. For many māhū, LGBTQIA+, and QTPI+ youth, especially those who are not "out" at home, mandating parental consent to access social media platforms may effectively cut off critical lifelines to affirming communities, mental health resources, and peer support networks.

Additionally, placing the burden of compliance on workers within app stores and technology companies, many of whom are already navigating complex and under-regulated digital environments, raises concerns about workplace implementation, enforcement, and potential liability. Without clear labor protections and standards, this bill risks shifting responsibility onto workers rather than addressing systemic accountability at the corporate level of the social media platforms where it belongs.

We are also concerned about the broad requirement for platforms to “identify young person users through their algorithms,” which could incentivize invasive data tracking practices and deepen existing concerns about algorithmic bias and discrimination. These systems are not neutral and have historically disproportionately impacted marginalized communities.

Rather than creating new systems for data collection and surveillance, we urge the Legislature to focus on policies that:

- Hold social media companies accountable for the spread of harmful misinformation;
- Strengthen data privacy protections for all users;
- Invest in digital literacy education to help young people critically evaluate online content; and
- Ensure any youth safety measures do not isolate or endanger vulnerable populations.

Protecting keiki online is a shared responsibility, but it must be done in a way that safeguards privacy, equity, and access to community. This bill shifts the responsibility to

For these reasons, Pride at Work – Hawai‘i respectfully urges the Committee to defer SB 2671 SD 2 HD 2.

Mahalo for the opportunity to testify.

In Solidarity,

Michael Golojuch, Jr. (he/him)
President
Pride at Work – Hawai‘i

CHAMBER OF PROGRESS

April 1, 2026

The Honorable David Tarnas
Chair
Committee on Judiciary and Hawaiian Affairs
Room 442, State Capitol
415 South Beretania Street
Honolulu, HI 96813

RE: Oppose SB 2761 - App Store Age Verification

Dear Chair Tarnas and members of the Committee:

On behalf of Chamber of Progress, a tech industry association supporting public policies to build a society in which all people benefit from technological advances, **I respectfully urge you to oppose SB 2761,** which would mandate intrusive age verification and parental consent requirements that undermine privacy, centralize sensitive personal data, and risk cutting young people off from essential online resources.

SB 2761 requires intrusive age verification that undermines privacy for all users

SB 2761 requires app stores to perform account-level age verification, effectively forcing the verification of the identity and age of all users, including adults. Strict age verification, which would require confirming a user's age without collecting additional personally identifiable information, is not technically feasible while still respecting users' rights, privacy, and security.[1] For example, an adult downloading a weather app, a banking app, or a news app would be required to submit identifying information to an app store despite posing no child safety risk. This places adults in the unfair position of having to surrender sensitive personal data as a condition of participating in the digital economy, contradicting core principles of privacy, data minimization, and user autonomy.

[1] Sarah Forland et al. *Age Verification: The Complicated Effort to Protect Youth Online*. Open Technology Institute, New America, Apr. 22, 2024. https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/

Centralizing age verification at the app store level creates systemic security and misuse risks

By concentrating sensitive age and identity data at the app store level, the bill creates a single, high-value target for data breaches, misuse, and cyberattacks. App stores would be required to maintain large-scale repositories of verified identity information, increasing the potential harm if that data is compromised.

This risk is not hypothetical. Past breaches of centralized identity systems have exposed millions of users to fraud, identity theft, and harassment. For example, the 2017 Equifax breach compromised sensitive personal data, including Social Security numbers, for roughly 147 million Americans,[2] while a 2024 breach at National Public Data,[3] a background check and data broker company, potentially exposed up to 2.9 billion records containing sensitive personal information such as full names, addresses, and Social Security numbers.

Additionally, in Hawaii, a 2025 ransomware attack on the University of Hawaii Cancer Center exposed highly sensitive personal information for approximately 1.2 million individuals, including Social Security numbers, driver's license data, and health-related information, illustrating the real-world consequences when centralized systems holding personal data are compromised.[4]

Under this framework, a single vulnerability at the app store level could expose sensitive information for vast numbers of users, including minors, magnifying the consequences of any failure.

SB 2761 responsibility away from developers best positioned to implement tailored safety measures

App developers are generally better suited than app stores to design and implement safety features that reflect the specific risks, content, and use cases of their services. The bill instead shifts responsibility to the app store layer, requiring app stores to share users' age categories with developers and mandating uniform age-based restrictions.

---

[2] "Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach." Federal Trade Commission, Jul. 22, 2019. https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach

[3] Nicole Tan. "2.9 billion records may have been exposed in a data breach. Here's what to know." NBC Washington, Aug. 15, 2024. https://www.nbcwashington.com/news/national-international/2-9-billion-data-records-may-have-been-exposed-in-a-data-breach-heres-what-to-know/3695197/

[4] Ionut Arghire. "1.2 Million Affected by University of Hawaii Cancer Center Data Breach." Security Week, Mar. 3, 2026. https://www.securityweek.com/1-2-million-affected-by-university-of-hawaii-cancer-center-data-breach/

For example, a social platform, an educational app, and a messaging service each present distinct safety considerations and already deploy different moderation tools, parental controls, and age-appropriate experiences. Imposing a one-size-fits-all model at the app store level risks weakening these platform-specific protections while relieving large services of accountability for how safety is actually implemented within their products.

Mandatory parental consent requirements risk harming teens in vulnerable or high-conflict households

SB 2761 requires minors under sixteen to obtain verifiable parental consent before they can download, purchase, or make purchases on social media platforms. Because access is conditioned on parental approval at the app store level, minors who are unable or unwilling to involve a parent are effectively barred from participating in large portions of the online ecosystem. While parental involvement can be beneficial in many contexts, blanket consent requirements do not account for the wide range of family dynamics and can be misused in high-conflict, unsupportive, or abusive households.

For example, teens seeking access to mental health resources, LGBTQ+ support communities, or educational tools could be blocked by a parent who is unsupportive or controlling. Research consistently shows that online engagement can reduce isolation and improve mental health outcomes for vulnerable youth, and policies that indiscriminately restrict access risk cutting off these critical lifelines.

SB 2761 prioritizes control over safety and risks unintended harm to young people

By emphasizing age verification and parental control over flexible, context-specific safety measures, the bill risks substituting compliance for meaningful protection. Restricting access through rigid consent mechanisms does not address the underlying causes of online harm and may instead push young people toward less visible or less regulated online spaces.

A more effective approach would focus on empowering developers to build age-appropriate experiences, improving digital literacy, and providing families with tools that support safety without requiring universal identity verification or blanket parental permission for ordinary app use.

Recent Texas ruling highlights constitutional problems with app store age verification mandates

SB 2761 follows a policy path that courts are already rejecting. In December 2025, a federal judge blocked Texas's app store age verification law as likely unconstitutional under the First Amendment, finding that the state failed to use the least restrictive means

to achieve its child safety goals and noting that existing parental control tools already allow families to manage children's app use without restricting lawful speech or requiring users to surrender identifying information.[5] SB 2761 adopts the same framework by requiring app stores to verify users' age categories and condition minors' app downloads and purchases on parental consent, relying on broad, account-level verification and default restrictions rather than targeted safety tools, and therefore raises the same legal and practical concerns that led the Texas law to be blocked before it could take effect.

Additionally, Utah is now facing a similar constitutional challenge. In February 2026, a lawsuit was filed seeking to block Utah's app store age verification law on First Amendment grounds, arguing that the state cannot require broad, account-level age gating and parental consent as a condition of accessing lawful apps.[6] This reinforces that courts are increasingly skeptical of app store age verification mandates as a constitutionally permissible approach to child safety.

For these reasons, **I respectfully urge you to oppose SB 2761.** While protecting young people online is a shared priority, this bill would erode privacy for all users, weaken platform-specific safety protections, and impose rigid consent requirements that risk harming vulnerable youth without meaningfully improving online safety.

Sincerely,

Robert Singleton
Senior Director of Policy and Public Affairs, California and US West

[5] "Judge Blocks Texas's App Store Accountability Act as Unconstitutional Speech Restriction." Computer & Communications Industry Association, Dec. 23, 2025 https://ccianet.org/news/2025/12/judge-blocks-texass-app-store-accountability-act-as-unconstitutional-speech-restriction/; "CCIA Challenges Unconstitutional App Store Law in Utah." Computer & Communications Industry Association, Feb. 5, 2026. https://ccianet.org/news/2026/02/ccia-challenges-unconstitutional-app-store-law-in-utah/

[6] "CCIA Challenges Unconstitutional App Store Law in Utah." Computer & Communications Industry Association, Feb. 5, 2026. https://ccianet.org/news/2026/02/ccia-challenges-unconstitutional-app-store-law-in-utah/

THE TREVOR PROJECT

For Young LGBTQ+ Lives

March 31, 2026

RE: Opposition to SB 2761 and impacts on LGBTQ+ young people

Dear Chair Tarnas, Vice Chair Poepoe, and members of the Judiciary & Hawaiian Affairs Committee,

The Trevor Project writes to express our opposition to SB 2761, which would require parental consent for young people under 16 to create or maintain a social media account, regardless of the nature or design of the platform. We urge you to oppose SB 2761 in its current form, which will prevent LGBTQ+ young people from accessing life-saving online support systems.

The Trevor Project is the leading suicide prevention and crisis intervention organization for LGBTQ+ young people. Trevor offers 24/7 crisis services, connecting highly trained counselors with LGBTQ+ young people whenever they need support. To drive prevention efforts, The Trevor Project also operates robust research, advocacy, education, and peer support programs. Finally, to support our mission of ending LGBTQ+ youth suicide, we have created TrevorSpace, the world's largest safe space social networking site designed specifically for LGBTQ+ young people ages 13-24. TrevorSpace is a moderated online community that provides a welcoming environment for young people to explore their identities, find peer support, and make friends.

We know from research – and from what LGBTQ+ young people tell our trained counselors at Trevor – that social media has the potential to cause harm. Social media can contribute to negative outcomes such as bullying, anxiety, depression, and eating disorders, and it's important that these issues are addressed through proactive measures. We applaud the intent behind SB 2761 to protect young people from the harms of social media.

However, we cannot ignore the reality that many LGBTQ+ young people – especially those who do not live in supportive homes or communities – turn to the internet to better understand themselves, and to find support and belonging. These online spaces can be life-saving; **LGBTQ+ young people with access to affirming online spaces report significantly lower odds of attempting suicide.** Properly designed and moderated, platforms like TrevorSpace have demonstrated the ability to bring youth together, connect them to the support they need, and even positively impact their mental health and well-being.

While SB 2761 aims to protect the mental health of young people, the amended requirement to require parental consent for young people under 16 to create or maintain social media accounts, regardless of the nature of the platform or safety of its design, does not take into account that different young people have different needs, and will especially cause unintended harm for LGBTQ+ young people who are at the highest risk. LGBTQ+ young people who do not feel safe or supported in their home or community often seek supportive spaces online, as well as information to better understand their identity. Requiring parental consent to create any social media account may force LGBTQ+ young people to choose between risking rejection and safety by having their identity inadvertently disclosed, or remain isolated without access to critical support systems and mental health support.

As the legislature considers legislation intended to make social media safer for young people, we hope you will take these unique experiences of LGBTQ+ young people into account and reject provisions that would strip them of life-saving online support systems. The relationship between social media and youth mental health is nuanced, and the solutions should be too, leaning into empowering social media users and their families to make their own decisions and to control their experiences online.

Given our hands' on experience with these topics, we are more than happy to help explore solutions that achieve our shared goal of a safer, more accepting online environment for all youth. Please do not hesitate to reach me at casey.pick@thetrevorproject.org to discuss this topic further.

Sincerely,

Casey Pick
Senior Director of Law & Policy
The Trevor Project

DATE: April 1, 2026
TO: Committee on Judiciary & Hawaiian Affairs
FROM: The Entertainment Software Association
RE: SB 2761 SD2 HD 2 – Oppose Unless Amended

Dear Chair Tarnas and Members of the Committee on Judiciary & Hawaiian Affairs,

On behalf of the video game industry, the Entertainment Software Association (ESA) writes to express serious concerns with SB 2761 SD2 HD2. Although well-intentioned, the bill's mandatory age-verification, combined with the broad definitions of app store and social media, is unworkable and would undermine the robust parental controls video game companies already provide. Notably, similar laws have not been successfully implemented elsewhere in the United States. If the goal of the legislature is to protect children from social media, then we recommend that the committee revert to SB2761 HD1. The new language being considered shifts the burdens of responsibility away from the social media companies. We respectfully urge this committee to revert the bill to SB2761 HD1.

First, SB 2761 SD2 HD2 is likely to conflict with the First Amendment. The only type of speech for which there is age verification online is content harmful to minors (i.e., sexually explicit content or pornography), and even then, a First Amendment analysis must still be performed because such a requirement impacts the speech rights of adults. Broad age verification measures enacted in Texas and Utah face legal challenges, with the Texas law already enjoined on First Amendment grounds, and a similar law passed in Louisiana is expected to be significantly amended before it becomes effective this summer.

Additionally, SB 2761 SD2 HD2 would require the extensive collection, processing, storage, and sharing of highly sensitive personal information, including government-issued identification and biometric data. Even with safeguards, requiring this information to be transmitted among app stores and developers creates substantial privacy and security risks. The bill would effectively link sensitive personally identifiable information to every user account, whether adult or minor. Concentrating this volume of sensitive data across multiple entities increases the risk of breaches and undermines broader national and global efforts to enhance data security and minimize data collection.

ESA respectfully urges the Committee not to advance SB 2761 SD2 HD2 in its current form. As written, the bill would force an over-collection of data and would likely not achieve the goals of the legislature. ESA and its members are committed to protecting all gamers online and stand ready to work collaboratively with the Committee to develop workable, balanced solutions in this complex and evolving policy area. Please do not hesitate to contact the undersigned with any questions.

Sincerely,

Andrew O'Connor
Director, State Government Affairs
Entertainment Software Association

ACT | The App Association

April 1, 2026

Hawai‘i House Committee on Judiciary and Hawaiian Affairs
Hawai‘i State Capitol
415 South Beretania Street
Honolulu, HI 96813

RE: SB 2761

Dear Chair Tarnas, Vice Chair Poepoe, and Members of the House Committee on Judiciary and Hawaiian Affairs:

On behalf of ACT | The App Association, I am writing to share concerns regarding SB 2761. ACT is a global trade association representing small and medium-sized technology companies and independent app developers that drive innovation, job creation, and economic growth across the country, including in Hawai‘i.

ACT and our members share your commitment to protecting children online and empowering parents with meaningful tools to manage their children's digital experiences. We take this responsibility seriously and support policies that genuinely improve online safety without unintentionally undermining privacy, innovation, or legal clarity.

However, SB 2761, as currently drafted, raises serious concerns, particularly for small app developers that build general audience products or services that may fall within the bill's broad definition of a social media platform. SB 2761 establishes broad compliance obligations that are extremely difficult to implement in practice. For example, the bill's requirements related to age assurance will likely necessitate building new or expanded technical infrastructure to comply. They may also trigger additional legal obligations under frameworks such as the Children's Online Privacy Protection Act (COPPA), even if the app is not designed for or marketed to children. For small developers, establishing and maintaining these systems is costly, complex, and often unrealistic. Unlike large multinational companies, small businesses do not have compliance teams or legal departments. As a result, some developers may limit features, restrict access for users, or leave the market entirely, reducing choice and innovation for consumers.

Second, SB 2761 would likely increase privacy and security risks. While well-intended, the bill's approach to age assurance mandates an entirely new data collection infrastructure that creates privacy and security risks by design. More data collection means more risk. Online safety is strengthened when companies collect less personal information, not more.

Finally, SB 2761 raises legal and constitutional concerns. Conditioning minors' access to lawful digital content on parental consent, regardless of whether data is collected, risks restricting protected speech. These concerns are real. Late last year, a federal court blocked enforcement of a similar Texas app store age verification law, finding it likely violated the First Amendment.

We share your goal of protecting children online. We believe that goal is best achieved through device-level parental controls, parental education, transparency, and alignment with existing federal frameworks, rather than sweeping mandates that place disproportionate burdens on small businesses. For these reasons, we respectfully urge you to oppose SB 2761.

ACT stands ready to work with lawmakers on solutions that are effective, privacy protective, and workable for the innovators serving Hawaiʻi families.

Thank you for your time and consideration.

Morgan Stevens
Policy Associate
ACT | The App Association

April 1, 2026

Hawaii House Committee on Judiciary and Hawaiian Affairs
Hawaii State Capitol
415 South Beretania St.
Honolulu, HI 96813

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

On behalf of the Computer & Communications Industry Association (CCIA), I write to Chair Tarnas, Vice Chair Poepoe, and Members of the House Committee on Judiciary and Hawaiian Affairs:

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

[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, 2026 WL 561099 (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).

laws.[13] As it is impossible to objectively determine which of an online service's purposes or 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

---

[13] *See, e.g.*, *Jones*, 2026 WL 561099 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.
[14] *Griffin*, 2025 WL 978607 at *36.
[15] *Id.* at *37.
[16] *Jones*, 2026 WL 561099 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.

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

SB 2761's regulations apply to individuals less than 16. Due to the nuanced ways in which children and teens use the internet, it is imperative to appropriately tailor such treatments to respective age groups. For example, a 15-year-old conducting research for a school project can be expected to encounter, 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.[24] 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.

* * * * *

While we share the concerns of the sponsor and the Committee 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 your consideration of these comments and stand ready to provide additional information as you consider proposals related to technology policy.

Respectfully submitted,

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

[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] *See* 15 U.S.C. § 6501(1) (1998).

STONEWALL CAUCUS
FORMED IN 2001

THE FIRST CAUCUS OF THE
DEMOCRATIC PARTY OF HAWAI'I

TESTIMONY IN OPPOSITION TO SB2761 SD2 HD2 (REQUEST TO DEFER)
Committee on Judiciary & Hawaiian Affairs (JHA)
Wednesday, April 1, 2026
2:00 PM

Aloha Chair Tarnas, Vice Chair Poepoe, and Members of the Committee,

My name is Abby Simmons, and I am the Chair of the Stonewall Caucus of the Democratic Party of Hawai'i. I am writing in **opposition to SB2761 SD2 HD2 and respectfully request that this measure be deferred.**

We recognize and share the Legislature's concern regarding youth mental health and the potential harms of social media. However, SB2761, as currently drafted, risks causing serious unintended harm, particularly to LGBTQ+ young people who rely on online spaces for safety, identity exploration, and access to life-saving support.

As outlined in the bill, SB2761 requires digital application stores to verify user age and mandates parental consent for individuals under sixteen to access social media platforms.
While intended as a protective measure, this requirement fails to account for the lived realities of many young people in Hawai'i.

For LGBTQ+ youth, especially those who are not supported or safe at home, requiring parental consent creates a dangerous barrier. It may force young people to disclose their identity before they are ready or safe to do so, or cut them off entirely from critical support networks. Many LGBTQ+ young people turn to online spaces precisely because they cannot access affirmation or understanding in their immediate environments.

Research underscores this reality. LGBTQ+ youth who feel safe and understood in at least one online space report significantly lower odds of attempting suicide. At the same time, a majority of LGBTQ+ youth report that their homes are not affirming environments, while a far greater percentage report feeling affirmed online.

This bill applies a one-size-fits-all approach to a complex and nuanced issue. Social media is not monolithic, platforms vary widely in design, purpose, and safety. Moderated, mission-driven spaces exist specifically to provide safe, structured, and affirming environments for vulnerable youth. SB2761, as written, does not distinguish between these types of platforms and large commercial social media companies.

Additionally, the bill creates broad compliance obligations for digital application stores and social media platforms, including age verification and data sharing requirements, that may disproportionately burden smaller platforms and nonprofit entities without improving outcomes for youth safety.
For these reasons, we respectfully urge the Committee to defer this measure.

If the bill is not deferred, we strongly urge amendments to mitigate harm and better target the Legislature's intent. Specifically, the definition of "social media platform" should be refined to:

• Exempt smaller entities and nonprofit platforms, including those that provide moderated, support-based services;

• Include revenue thresholds (for example, limiting applicability to entities exceeding $100 million in annual revenue, including revenue derived from advertising or the sale of personal data);

• Include meaningful user-base thresholds to ensure that only large-scale platforms are covered (for example, a high statewide user threshold such as 300,000 users in Hawai‘i or a comparable national threshold);

• Ensure that platforms whose primary purpose is peer support, crisis intervention, or community safety are not unintentionally restricted.

These amendments would help ensure that legislation aimed at protecting youth does not instead isolate those who are most vulnerable.

Hawai‘i has long been a leader in protecting LGBTQ+ people and advancing policies grounded in care, dignity, and inclusion. We have an opportunity here to take a thoughtful, evidence-based approach that protects young people without cutting them off from the support systems they rely on.

For these reasons, the Stonewall Caucus respectfully urges the Committee to defer SB2761 SD2 HD2. Mahalo for the opportunity to testify.

Respectfully submitted,

Abby Simmons (she/her)
Chair
Stonewall Caucus of the Democratic Party of Hawai‘i

KOBAYASHI SUGITA & GODA, LLP
Attorneys at Law

March 31, 2026

COMMITTEE ON JUDICIARY & HAWAIIAN AFFAIRS
Rep. David A. Tarnas, Chair
Rep. Mahina Poeopoe, Vice Chair

HEARING DATE: April 1, 2026
TIME: 2:00 p.m.
PLACE: Conference Room 325

Re: TESTIMONY ON BEHALF OF META OPPOSING SENATE BILL 2761, SD2, HD2

Dear Chair Tarnas, Vice Chair Poepoe, and Members of the Judiciary & Hawaiian Affairs 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. And we applaud Senator Keohokalole and the legislature for recognizing that age assurance and parental consent should take place at the App Store level–which allows for an easier and more privacy-protective process for parents to monitor their children's social media use. Overall, this 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.

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 assurance and parental consent should occur at the app store level, we want to be clear that Meta invests heavily in teen safety. In recent years, we rolled out Teen Accounts for Instagram, Facebook, and Messenger—a 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 13+ movie rating criteria and parent feedback 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.

Although we appreciate that this bill now places age assurance and parental consent at the App Store level, we are concerned that it applies only to social media apps because it makes the bill less empowering for parents and leaves it open to constitutional challenge. Teens these days are using an average of over 40 apps per week. Applying the bill to more apps would empower parents to have more control over the breadth of their teens' online experiences -- beyond only social media. It would also allow more apps to provide age-appropriate experiences, because they would be able to receive a reliable age signal from an app store and apply it to differentiate their experiences. Courts across the country have held that age assurance and parental consent requirements targeting social media companies violate the First Amendment; these courts have found these laws to be content-based restrictions that cannot survive strict scrutiny. This is in part because there are other apps–such as entertainment or streaming services—that utilize the same features as social media (including algorithmic ranking of content), but would not be captured in the legislation. Accordingly, we recommend expanding the scope of this bill to include *all* apps, and avoiding a scope that raises constitutional concerns.

We are further concerned that vague language in the bill requiring platforms to "identify young persons" using algorithms "and verify the user's age" would require age verification at the app store *and* on an app-by-app basis. 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. The bill should clearly centralize age assurance and parental consent at the app store level and remove language that contradicts the app store approach.

An app-by-app mandate would require parents to repeat the same steps across all the social media apps their teens use. 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.

An 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 agree that apps have a role to play in age assurance, and they should use the information available to them through their business. But requiring each app to independently verify age would be overly burdensome for parents.

We appreciate the direction of the bill's recent amendments, which reflect that the App Store is the best place for age assurance and parental consent. Please find language attached below that would address the issues outlined in our testimony. We look forward to partnering with you to help keep kids safe online.

Very truly yours,

DAVID M. LOUIE
for
KOBAYASHI SUGITA & GODA, LLP

S.B. NO. 2761, S.D. 2, H.D. 2

THE SENATE
THIRTY-THIRD LEGISLATURE, 2026
STATE OF HAWAII

A BILL FOR AN ACT

RELATING TO SOCIAL MEDIA.
BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:
SECTION 1. The legislature finds that social media companies function by compelling their users to spend as much time as possible on their platforms. By generating revenue from advertising on their platforms, social media companies operate under a model that encourages optimization for users' time spent on the platform and resist any platform changes, including safety changes, that could decrease stay time because every minute spent on the platform increases profitability and the company's bottom line.
The legislature further finds that social media companies employ a variety of features described as coercive design tactics, which foster psychological dependence and take advantage of the same dopamine-inducing strategies employed by the gambling industry to make the platform as addictive as possible and keep users returning and spending as much time as possible on the social media platform. These tactics are particularly harmful to children because children have minimal ability to self-regulate effectively and lack executive function to control their screen time.
The legislature further finds that the United States Surgeon General's Advisory of 2023 states that the nation is experiencing a "youth mental health crisis". The United States Surgeon General noted that despite some social benefits, numerous studies suggest that social media use presents a profound risk of harm to the mental health and well-being of children and adolescents. Factors such as the amount of time children and adolescents spend on social media platforms, the type of content and interactions children and adolescents experience, and disruptions to other activities essential for health, such as sleep and exercise, can play a complex role in the impact of social media on an individual child's or adolescent's mental health. The United States Surgeon General also expresses serious concern with the way social media is designed, deployed, and utilized while the outcomes for today's generations of children and adolescents remain unknown.
The legislature also finds that some social media companies have implemented age verification systems and made other efforts to protect minor users. However, the legislature believes these actions to be inadequate. Reporters and nonprofits have been able to create fake accounts that allow them to pass as children and children have no problem creating fake accounts that allow them to pass as adults.
The legislature further finds that digital application stores may be better positioned to verify the age of an account holder. By requiring age verification at the level of the digital application stores, there will be a single point of verification rather than several fragmented, less effective

checks by multiple social media platforms, will operate as a preventive measure by preventing minors from accessing social media platforms, rather than trying to restrict a minor's access after the fact.

The legislature further finds that the State has a compelling interest in protecting the physical and psychological well-being of minors. However, 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.

Accordingly, the purpose of this Act is to, under the laws regarding unfair or deceptive acts or practices:

(1) Require a digital application store provider to verify the age of users, require parental consent for users under sixteen years of age to download or purchase, or make a purchase on, a social media platform, and distribute that information to social media platforms; and

(2) Require social media platforms to obtain the age information from digital application store providers, determine whether parental consent has been provided for young persons, and take reasonable steps to identify young person users through their algorithms.

SECTION 2. Chapter 481B, Hawaii Revised Statutes, is amended by adding a new section to part I to be appropriately designated and to read as follows:

"§481B- Digital application stores; social media platforms; users under sixteen years of age; parental consent.

(a) A digital application store provider shall:

(1) At the time an individual who is located in the State creates an account with the digital application store provider:

(A) Request age information from the individual; and

(B) Verify the individual's age category using methods that are reasonably designed to ensure accuracy;

(2) If the age verification method determines the individual is a child or a young person, obtain verifiable parental consent before allowing the child or young person to:

(A) Download an application ~~social media platform~~;

(B) Purchase an application ~~social media platform~~; ~~or~~

(C) Make ~~a~~ purchases on an application ~~social media platform~~;

(3) Provide to a developer of an application ~~social media platform~~, in response to a request authorized under subsection (b):

(A) Age category data for a user located in the State; and

(B) The status of verified parental consent for a child or young person located in the State; ~~and~~

(4) Notify a developer of an application ~~social media platform~~ when a parent revokes parental consent ;and

(5) For pre-installed applications:

(A) Provide available age category information in response to a request from a developer; and

(B) Take reasonable measures to facilitate verifiable parental consent for use of the application in response to a request from a developer.

(b) A developer of an application ~~social media platform~~ shall:
(1) Verify through the digital application store provider's data sharing methods:
(A) The age category of users located in the State; and
(B) For a child or young person account, whether verifiable parental consent has been obtained;
(2) Request personal age category data or parental consent:
(A) At the time a user:
(i) Downloads an application ~~social media platform~~; ~~or~~
(ii) Purchases an application ~~social media platform~~; or
(iii) Launches a pre-installed application for the first time; or
(B) To comply with applicable laws or regulations.

(3) Take reasonable steps to identify child and young person users through the developer's available ~~social media platform's~~ algorithms and verify the algorithmically-identified potential young user's age to determine whether the user is subject to paragraph (4); and
(4) Not permit any individual the developer ~~social media platform~~ knows to be a child or a young person to be an account holder unless the individual has verifiable parental consent.
(c) Any violation of this section shall constitute an unfair or deceptive act or practice in the conduct of trade or commerce within the meaning of section 480-2.

(d) For the purposes of this section:
"Age category" means one of the following categories of individuals based on age:
() "Child," which means an individual who is less than thirteen years of age;
(1) "Young person", which means an individual who is at least thirteen and less than sixteen years of age;
(2) "Older teenager", which means an individual who is at least sixteen years of age and under eighteen years of age; or
(3) "Adult", which means an individual who is at least eighteen years of age.
"Age category data" means information about a user's age category that is collected by a digital application store provider and shared with a social media platform.
"Application" means a software application or electronic service that a user may run or direct on a mobile device.
"Child account" means an account with a digital application store provider that is established by an individual who the digital application store provider has determined is under thirteen years old through the digital application store provider's age verification methods."
"Developer" means a person that owns or controls an app made available through an application store or an application pre-installed onto a mobile device.
"Digital application store" means a publicly available website, software application, or electronic service that distributes applications from third-party social media platforms to users.

"Digital application store provider" means a person that owns, operates, or controls a digital application store that distributes applications to users in the State.
"Social media platform" means a public or semi-public internet-based service or application that allows users to view content generated by other users or create content viewable by other users of the platform's applications, in any format, including but not limited to text, pictures, and videos, through a landing page, main feed, gaming environment, or other surface, and that ~~primarily~~ serves as a medium for users to interact with content generated by other users of the platform; provided that no service or application that exclusively provides email or direct messaging services shall be considered to meet this criterion on the basis of that function alone.
"Pre-installed application" means any application, or portion thereof, that is present on a mobile device at the time of purchase, initial activation, or first use by the consumer, including browsers, search engines, and messaging, but excluding core operating system functions, essential device drivers, and applications necessary for basic device operation such as phone and settings. Pre-installed applications include applications, or portions thereof, installed or partially installed by the device manufacturer, wireless service provider, retailer, or any other party prior to purchase, initial activation, or first use by the consumer and which may be updated thereafter.
"Verifiable parental consent" means authorization that:
(1) Is provided by an individual who the digital application store provider has verified is an adult;
(2) Is given after the digital application store provider has clearly and conspicuously provided the parental consent disclosure to the individual; and
(3) Requires the parent to make an affirmative choice to:
(A) Grant consent; or
(B) Decline consent.
"Young person account" means an account with a digital application store provider that is established by an individual who the digital application store provider has determined is under sixteen years old through the digital application store provider's age verification methods."
SECTION 3. This Act does not affect rights and duties that matured, penalties that were incurred, and proceedings that were begun before its effective date.
SECTION 4. New statutory material is underscored.
SECTION 5. This Act shall take effect on January 1, 2077.

Report Title:
Digital Application Store Providers; Social Media Platforms; Individuals Under Sixteen Years of Age; Age Verification; Parental Consent; Unfair or Deceptive Acts or Practices
Description:
Requires a digital application store provider to verify the age of users, require parental consent for users under sixteen years of age to download or purchase, or make a purchase on, a social media platform, and distribute that information to social media platforms. Requires social media platforms to obtain the age information from digital application store providers, determine whether parental consent has been provided for young persons, and take reasonable steps to identify young person users through their algorithms. Effective 1/1/2077. (HD2)

Testimony In Opposition To SB2761_HD2

March 31, 2026

Part I: Greetings and Introduction

Dear Committee Members,

Thank you for listening to my testimony. While I do recognize some attempt to address some of the excesses of SB2761 in the previous hearing, the main underlying problem of invasive age-verification (AV) remains. In the current SB2761_HD2, AV is required for app stores which, according to the bill, is any website or online service that allows a download of an app for a social media platform. AV requires scanning photo IDs, sensitive financial documents, and a biometric face scan that is uploaded to third-party AV service and/or the online platform/application/store itself. The bill requires social media platforms to remove users under the age of 16 by identifying those minors through data from the app store's AV and from data collected from the social media's algorithm. The problem here is that data from algorithms often lead to mistakes where adult users are flagged as minors. As an example, adult social media users who do not view or interact with mature content could all have their account terminated because the algorithm could interpret such behavior as that of a minor. YouTube has imposed similar AV based on AI analysis of algorithm data which has led to many adult users being erroneously misidentified as minors and locked out of important site features unless they go through AV that requires ID and face scans.[1] Invasive AV would need to be employed to correct mistakes made by algorithm data. There is also the problem of numerous small web forums, image posting sites, and more that are considered as social media by the bill, but do not have apps that can be downloaded from app stores, do not employ algorithms, and cannot afford AV. Hawaii residents and visitors could be left with an internet only comprised of the massive and predatory social media and Big Tech giants while smaller sites and would-be competition that many rely on would become inaccessible as they are forced to block the state because they cannot comply with the law. As a Hawaii resident who will have to live under this law, I strongly oppose SB2761_HD2 and I strongly urge this committee to also oppose the bill.

Part II: Age-Verification Hurts Artists, the Poor, the LGBTQ+ Community, 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 and other restrictions that SB2761_HD2 will impose. I share my art on small niche art posting websites that are considered as social media by this bill. These small websites do not have an app for their site, do not employ algorithms, and cannot afford AV. Therefore, if SB2761_HD2 becomes law, I would be locked out from using these sites as there is no possible way for them to comply with the law and would, therefore, be necessary to block users from Hawaii. I am deathly afraid that my time as an artist maybe coming to an end because SB2761_HD2 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[2]. 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: Age-Verification Harms the Kids and Teens it is Supposed to Protect

Beginning with the previous SB2761_HD1, the bill has made attempts to address the issue of violating the First Amendment free speech rights of minors. In SB2761_HD2, there are provisions that allow minors to use app stores and social media, provided they have explicit expressed parental permission. But these revisions still do not respect the free speech rights of kids and teens. First of all, it is still adults who get to decide whether their children should be allowed to exercise their free speech rights as they need parental permission; in essence, SB2761_HD2 still restricts First Amendment rights for kids and teens by handing it over to their parents. In many cases, this may not be much of a problem for parents who do have their children's best interest in mind; however, this maybe a dangerous problem for children whose parents do not have their best interest in mind, such as in cases of neglect and abuse. Beyond such cases, parents who may want to allow their children to use social media still may be deterred. This is because of AV as it is now the parents would need to put their ID documents and face at risk of being leaked to the public and become a victim of identity theft from insecure AV. Related to this, as teens aged 16 and 17 are allowed to use social media, the AV mandate would require them to also endanger their own ID documents and face to the same risk of data breaches and identity theft parents and adults face. Finally, kids within the foster have absolutely no recourse to use app stores or social media as they do not have parents or guardians who can give them permission. SB2761_HD2'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.

Locking out minors from social media does harm them. 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.[3] 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.[4] 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 themselves as they who will 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).[5] 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.

Part IV: Age-Verification Is An Inherent Privacy Problem

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)[6], the chat service Discord (70,000 users had their IDs exposed)[7], 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)[8]. 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.[9] As this is nearly 2/3 of the entire population of the US, it is likely that I as well as members of this committee have been

affected by this. AV services and social media platforms cannot protect the sensitive private data they are required to collect.

The privacy problem of AV cannot be resolved by legislation. In fact, AV legislation is a root cause of AV's privacy nightmare. As long as AV laws require internet platforms and AV services to prove they are ensuring minors do not access to social media and other restricted content/services, they must always keep records to prove compliance to law enforcement and government threatening to punish them for noncompliance. That means these companies must keep ever growing databases full of photo ID scans, biometric face scans, and sensitive financial documents that can never be erased which in-turn, become ever more difficult secure and an ever more lucrative target for hackers.

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.[10] 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.[11]

Part V: The Experts' Warning Against Age-Verification

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.[12] 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 (like YouTube's AI-based AV and the algorithm-based AV proposed by SB2761), 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 distress 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.

Part VI: Age-Verification 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, become permanently blocked in US District Court for the Middle District of Louisiana back in mid-December.[13] The most serious judgment 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. AV mandates are 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 previous testimonies of the Department of the Attorney General and the Department of Commerce and Consumer Affairs.

As SB2761_HD2 has introduced an AV mandate on app stores, similar laws have also been found to be potentially unconstitutional. On December 23rd, Texas' app store AV law, SB2420, became blocked by preliminary injunction in Computer and Communications Industry Association (CCIA) v. Paxton.[14] The judge considered the law to be as unconstitutional as requiring real life bookstores to verify the ages of every customers before entering and then requiring customers who are minors to gain parental consent before entering to make a purchase.[15]

Part VII: Age Verification and Social Media Restrictions May Inhibit 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. Governor Josh Green has used social media, like Facebook and Instagram, to post up important information about those recent storms such as satellite tracking and emergency radio stations; as Facebook and Instagram both require users to have accounts to browse most the site, should SB2761_HD2 become law, Hawaii users would need to go through AV via the app store for their mobile app or be subjected to AV later if their account in flagged as that of a minor. 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_HD2 result in a mass departure of Hawaii users off of major social media platforms (whether they are kicked off by being mistakenly flagged as minors and/or will not or cannot go through AV), 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 VIII: 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_HD2, ironically, empower Big Tech more than ever. Should SB2761_HD2 become law, smaller websites are simply shut out of Hawaii completely while large social media platforms with their pervasive mobile apps and predatory algorithms 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_HD2. Thank you for your time, consideration, and hard work.

Sincerely,
Cary

1 An article from Tom's Guide discussing YouTube's rollout of its AI-based AV and mentioning users flagged as minors by mistake: https://www.tomsguide.com/computing/online-security/youtubes-ai-powered-age-verification-is-back-heres-what-that-means-for-you

2 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

3 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

4 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

5 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

6 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/

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

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

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

10 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

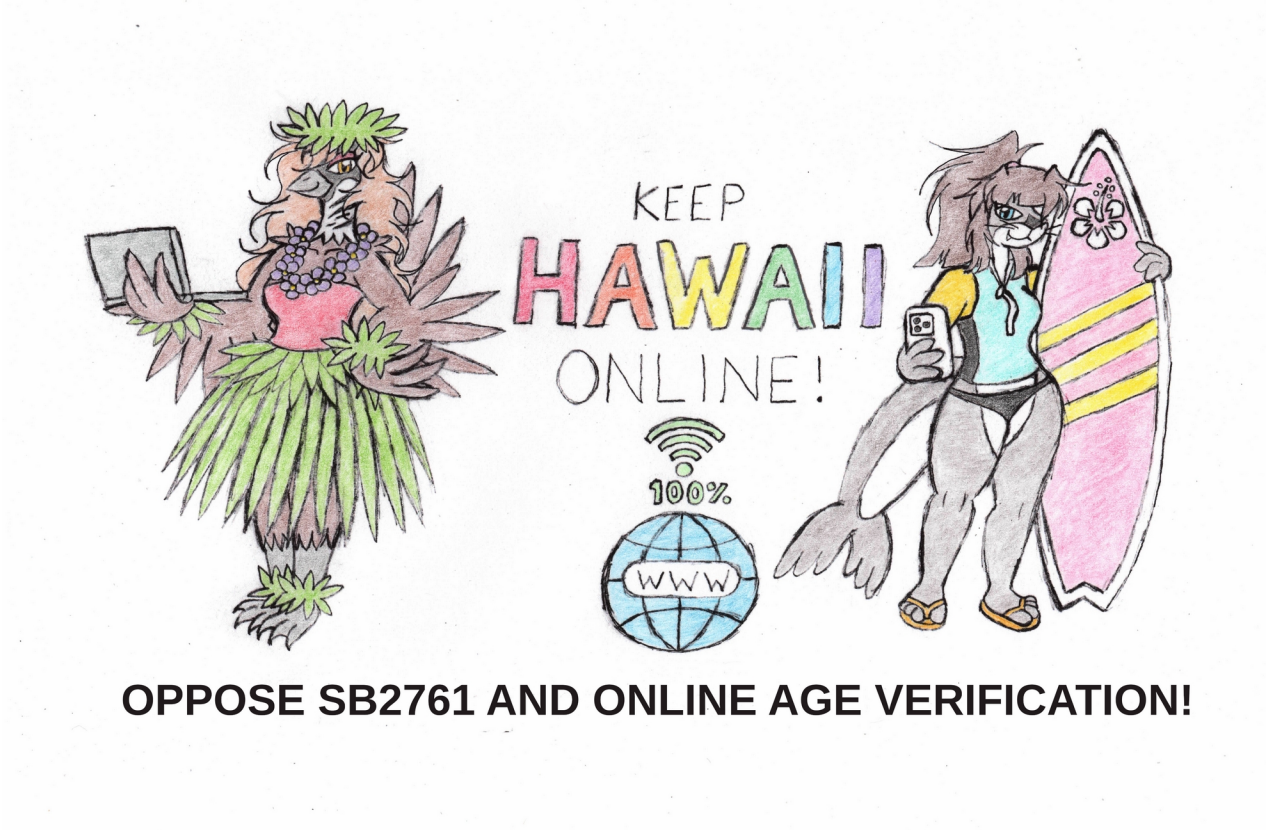
11 The Rage's article about AV service Persona's mass surveillance of its users: https://www.therage.co/persona-age-verification/

12 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/

13 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/

14 The Computer and Communications Industry Association's (CCIA) press release about the preliminary injunction in CCIA v. Paxton: https://ccianet.org/news/2025/12/judge-blocks-texass-app-store-accountability-act-as-unconstitutional-speech-restriction/

15 The Verge's article about CCIA v. Paxton: https://www.theverge.com/news/849752/texas-app-store-accountability-act-age-verification-injunction



Testimony in Opposition to SB2761 HD2

Dear Members of the Committee:

I am writing to respectfully voice my opposition to SB2761, version HD2. While the successive revisions of this bill have modified it on the margins, they have not ameliorated the fundamental problem: It impedes young people's access to constitutionally protected speech, with no care given to identify which Internet platforms are harmful and why. As an operator of an independent, nonprofit social-media forum that focuses on critiquing the excesses and evils of the tech industry, I must respectfully carry over my objections from my testimony in opposition to earlier versions. I have been trying to steer people away from "Big Tech" since long before that became politically fashionable. Indeed, it is difficult not to take a measure of personal offense at the fact that after multiple revisions, this bill still treats people like me the same as it treats Instagram and TikTok.

The bill's preamble recognizes the importance of "enabling minors to engage in constitutionally protected speech". But the bill itself does nothing to tailor its interventions narrowly enough to do that.

I. OVERBROAD SCOPE

Consider the bill's definition of "social media platform":

> a public or semi-public internet-based service or application that allows users to view content generated by other users or create content viewable by other users of the platform's applications, in any format, including but not limited to text, pictures, and videos, through a landing page, main feed, or other surface, and that primarily serves as a medium for users to interact with content generated by other users of the platform; provided that no service or application that exclusively provides email or direct messaging services shall be considered to meet this criterion on the basis of that function alone.

This encompasses virtually any website that makes user-generated content available at all. This includes not just those few companies implicated by the legislature's stated intent, but also the following:

- Discussion forums for niche interests (crochet, identifying local plants, discussing a favorite obscure TV show, etc.), that are run by volunteers, take no measures to monopolize attention or prolong the time users spend there, run minimal to no advertising, and could not by any stretch of the imagination be considered harmful to teenagers.
- Archive Of Our Own (AO3), a nonprofit website that hosts fanfiction and provides users with the ability to comment upon, bookmark and send kudos to the works of other users.
- Scirate, a nonprofit website where scientists and mathematicians bookmark and comment upon technical publications that have yet to be formally peer reviewed.
- Github, the primary platform for sharing and collaborating upon open-source software.

- Stack Exchange, a network of user-driven Q&A websites on many topics that began with computer programming and has since expanded to include subjects across the sciences and the arts.
- LibriVox, a platform where volunteers create and share audiobooks made from works in the public domain.
- Goodreads, a website where readers of books share their thoughts about them.
- Wikipedia, the free online encyclopedia made entirely of user-generated content, which against the odds has emerged as an example of the Internet doing something right, providing both reliable information and a valuable starting point for in-depth research.

Nearly all content on the Web is, at some level, *interactive*; indeed, this has been a selling point of the technology since its invention.[1] If one reads the bill's definition broadly enough that it encompasses the sites intended by the legislature (Facebook, TikTok and their ilk), then it inevitably encompasses benign sites too. One uses Facebook, for example, by scrolling through a feed and occasionally clicking an icon or leaving a reply. This is *the same kind and degree of interactivity* as provided by AO3 or Wikipedia. On Wikipedia, one scrolls through articles, clicks on links and pictures, edits article text, and comments on discussion pages. It is just not possible to take the words of the bill and draw a line that includes Instagram while excluding Wikipedia. This is the inevitable consequence of trying to regulate all communication platforms without regard to their size, amount and sources of income, and purpose.

The fundamental problem with SB2761 in all its versions is that it attempts to penalize an entire communications medium because of the bad behavior of two or three companies. In so doing, it strangles the possibilities for a better Internet, and it harms those it is meant to protect.

II. VAGUENESS AND THE SHELL GAME OF VERIFICATION BURDENS

The bill requires all websites in its fantastically broad remit to "Take reasonable steps to identify young person users". The bill does not specify what the limits of "reasonable steps" are, nor how the government of Hawaii will be making the determination of what counts as "reasonable". Websites ranging from birdwatcher forums to Wikipedia will be forced into a state of uncertainty: How much must they do in order to comply? How far must they go to avoid liability? The bill has been revised to shift the burden to app stores, but what about social media platforms that exist as *websites,* with no associated app and thus no app store to contact? Will hobbyist discussion forums that run on a shoestring budget then be forced to line the pockets of the age-verification industry and compromise the privacy of their users in the process?

Moreover, transferring the burden to app stores merely transfers the privacy problem, too. The bill's language indicates that self-attestation of age is insufficient (2(1)(B)). What are these "methods reasonably designed to ensure accuracy"? Having app stores demand *papers,*

[1] See, e.g., the discussion of "hot spots" and "live links" in Tim Berners-Lee's original 1989 proposal: `https://www.w3.org/History/1989/proposal.html`.

please is no better than having platforms do so. This is not a theoretical concern: Last October, hackers broke into the service that the Discord platform used for age verification and stole the government-issued IDs of 70,000 people.[2] SB2761 would not protect minors. On the contrary: It would put all citizens of Hawaii at risk for identity theft.[3]

As with age verification, so too for parental consent. The burden is on app stores to establish it, and the blunt economic truth is that only app stores owned and run by Big Tech will be able to do it. A small player, like a purveyor of open-source software, will be forced to quit the state entirely.

Denise Paolucci, co-owner of Dreamwidth Studios, has testified on this before a court of law:

> From my twenty-two year career in online Trust and Safety, I know that familial relationships are often far more complicated than conventional wisdom believes, and identifying which person is a minor's parent or guardian with legal decision-making authority is often a complex task. For instance, if a minor has two divorced parents who disagree about whether their minor child should be permittedt ohold an account on a website, the website must confirm the legal relationship between the parties and the minor involved, and determine which of the people at hand has the legal decision-making authority to provide sufficient parental consent. In a particularly contentious divorce, this can require a website to review divorce decrees, examine legal paperwork, and determine the authenticity and provenance of the documents supplied to them. Because someone who lives in [one state] may have obtained their divorce from any one of the thousands of courts across the United States, or even from another country, before moving to [that state], this would require us to become experts in authenticating and interpreting court documents from anywhere in the world to verify which parent has legal authority to provide parental consent. We do not have the capacity to perform this authentication, nor do we have the financial resources necessary to increase staffing to increase that capacity.
>
> [. . .]
>
> There is no national identity database that allows someone to verify a minor's identity, the legal relationship between a parent and a minor, or which parent has the authority to make binding decisions for a minor. There is no way to verify a user's identity beyond requiring the upload of government-issued identifying documents with corroborating photo or video confirmation, and many minors do not have photo ID. There is no way for a website to authenticate or verify that the documents uploaded for identity verification purposes belong to the person who is uploading them, that the person who controls the account is the same person who provided the identifying documents, or that the documents are legitimate and not a forgery. Disputes about the identity of an account holder,

[2] A. Belanger, "Discord faces backlash over age checks after data breach exposed 70,000 IDs," *Ars Technica,* 9 February 2026.

[3] Rep. Alexandria Ocasio-Cortez recently put the issue in appropriately stark terms: "Republicans are using kids as a smokescreen for what Big Tech lobbyists want: a national surveillance program to harvest our data with zero protections for people and their privacy." `@ocasio-cortez.house.gov` on Bluesky, 5 March 2026.

> their age, or the legal relationship between them and the person claiming to be their parent are complex, time-consuming, costly to investigate and resolve, and unfortunately common. [A social media ban for youth] would only increase their number. We do not have the capacity to accept this additional support burden, nor do we have the financial resources necessary to increase staffing to increase that capacity.[4]

And, of course, any documents uploaded in such a process are potential targets for identity theft.

III. HARMS WORSENED BY THE BILL

I share the grave concerns about this bill's impact on LGBTQ youth raised by theearlier testimony of Cary and of the Trevor Project. Giving parents who do not accept teenagers' gender identities or sexual orientation a chokehold over those teenagers' ability to find supportive community is a surefire way to ruin lives.

Forbidding young people from creating accounts on social-media platforms has another downside. Some platforms, such as YouTube, can be used passively without creating an account: One can watch videos on YouTube without logging in, but not comment upon them or upload one's own. Pushing young people in the direction of being passive content consumers rather than active participators in open conversation cannot be a good move for their development. Moreover, platforms may provide specialized environments or versions meant to be age-appropriate, like YouTube Kids. Perversely, preventing young people from creating accounts will throw them into the deep end of the pool, ensuring that their only experience of a site like YouTube will be one with far less moderation.

IV. CONSTITUTIONAL ISSUES

There are serious Constitutional issues with this bill. First and foremost, it evidently bars young people from websites that offer nothing obscene. And obscenity is the dividing line for where age verification can pass Constitutional muster.[5] Likewise, the bill runs directly into the Commerce Clause of the United States Constitution. It imposes requirements on the activity of persons entirely outside the state of Hawaii. Any platform outside of the state must still build the reporting and monitoring infrastructure to detect whether a user is covered. A resident of New York, accessing a platform hosted in Massachusetts, must sacrifice their anonymity to comply with a law that none of their elected representatives could have voted for. Because the law would have "the impermissible practical effect of

---

[4] Declaration of Denise Paolucci in Support of Plaintiff NetChoice's Motion for Preliminary Injuction, via `https://dw-news.dreamwidth.org/44429.html`.

[5] See *Free Speech Coalition, Inc. v. Paxton,* 606 U.S. 461 (2025), where the majority and minority opinions agreed that "for fully protected speech, the distinction between bans and burdens makes no difference to the level of scrutiny" (internal quotation marks omitted). See also *Moody v. NetChoice, LLC,* 603 U. S. 707 (2024); *Brown v. Entertainment Merchants Assn.,* 564 U. S. 786 (2011); and *NetChoice v. Fitch,* 606 U.S. __ (2025), J. Kavanaugh concurring in denial of certiorari.

controlling commercial activity wholly outside" Hawaii, it goes beyond what the Commerce Clause can allow.[6]

In addition, many terms and provisions are sufficiently unclear that the law is open to being ruled void for vagueness. Above, I noted the vagueness of "reasonable steps", but "primarily" and even "user" raise the same problem. Is a user necessarily an account holder? How prominent must a function be to make it the primary one? An issue like this demands more careful drafting.[7]

Moreover, the bill regulates how platforms must interact with users aged 13 to 15. This is contrary to the intent of Congress as codified into federal law, namely to regulate interactions with users younger than 13. The provisions of this bill could only become consistent with federal law if the Children's Online Privacy Protection Act were amended.

V. CONCLUSION AND ALTERNATIVES

The bill's description of the legislature's intent does not make a case for regulating all user-generated content, and the rationale it does provide is based on a slanted presentation of the facts. For example, research more recent than 2023 suggests that among young people, *moderate* social-media use is associated with better mental health than either heavy use or no use at all.[8] Correlation is not causation; heavy social-media use can be a consequence of poor mental health (e.g., seeking distraction) rather than a cause. The world has gotten worse for teens in many ways, from the vanishing of "third spaces" to the failure of institutions to care about providing a livable future, and pointing the finger at social media alone is burying one's head in the sand.[9] The social and psychological factors at work are interrelated, complicated, and difficult to study:

> Despite a wealth of research on this topic, the evidence base is currently limited in several important respects. These include primarily cross-sectional work that does not warrant causal conclusions; use of small and homogeneous samples; failure to control for confounding factors (e.g., gender); and, in the case of social media research, a predominant focus on total time spent as opposed to *how* that time is used. Finally, with a handful of exceptions, research to date has also not distinguished between-person (i.e., stable differences between individuals)

---

[6] *Healy v. Beer Institute, Inc.,* 491 U.S. 324 (1989).

[7] Per *Connally v. General Constr. Co.,* 269 U. S. 385, 391 (1926): "[A] statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application, violates the first essential of due process of law". And per *FCC v. Fox Television Stations, Inc.,* 567 U.S. 239 (2011): "Even when speech is not at issue, the void for vagueness doctrine addresses at least two connected but discrete due process concerns: first, that regulated parties should know what is required of them so they may act accordingly; second, precision and guidance are necessary so that those enforcing the law do not act in an arbitrary or discriminatory way. [. . .] When speech is involved, rigorous adherence to those requirements is necessary to ensure that ambiguity does not chill protected speech."

[8] B. Singh et al., "Social Media Use and Well-Being Across Adolescent Development," *JAMA Pediatrics* 180 (2026), 288–97.

[9] J. Severs, "Is Jonathan Haidt right about smartphones?" *Times Educational Supplement,* 3 September 2025.

> from within-person (i.e., situational changes within individuals) effects. This is critical because failure to do so can lead to erroneous conclusions regarding the presence, predominance, and sign of causal influences.[10]

This is not a good area in which to make blunt legal interventions. Complicated problems call for careful, flexible solutions.

I do not want to downplay the seriousness of young persons' use of social media. I have grave objections to the ways in which all of the largest social-media corporations behave, and I personally avoid all interactions with commercial social media to the fullest extent possible. I have opposed "Big Tech" for years, and I am writing out of concern that misguided attempts to regulate them will in fact entrench them. (Notice how the most recent revision of the bill has done Meta's bidding by shifting the burden onto app stores?[11]) I wish to underline that, to address the issue, we must first diagnose it properly, and then we must go about solving it in a targeted and principled way. For example, talk of "social-media addiction" is well nigh ubiquitous, yet research suggests that portraying bad social-media habits as "addiction" makes those habits harder to break.[12] No one benefits when we boil our problems all down to "dopamine".[13]

There are better alternatives than the approach taken here. Multiple aligned pushes in the same direction can be more effective than a single blunderbuss of an intervention. We can put a tax on targeted advertising. We can pass a strong privacy law that protects people of all ages, short-circuiting the toxic business models of giant corporations without "destroying the village in order to save it" by forcing platforms to gather data before deciding what amount of privacy they can offer. Consider a "youth center" model of reform, where we address the harms of the worst social-media platforms by giving teens better things to do on their phones. (Any minute spent playing a *Carmen Sandiego* game is a minute not spent on Instagram.) We can encourage independent and nonprofit social media by directing young people to platforms like Dreamwidth, Bluesky and Mastodon, platforms that aren't out to exploit them. We can educate parents about the safety features that already exist yet are under-utilized. As lawmakers, you can take a stand yourselves and cease using X and Meta, at once sending the message that we can live without these companies and broadening your own horizons about what the Internet has to offer.

Yours,
Blake C. Stacey, PhD
Co-moderator, TechTakes
Boston, MA
bstacey@mit.edu

---

[10] Q. Cheng et al., "How do social media use, gaming frequency, and internalizing symptoms predict each other over time in early-to-middle adolescence?" *Journal of Public Health* 48 (2026), 59–69.

[11] See https://old.reddit.com/r/linux/comments/1rshc1f/i_traced_2_billion_in_nonprofit_grants_and_45/ and Meta's previous testimony.

[12] I. A. Anderson and W. Wood, "Overestimates of social media addiction are common but costly", *Scientific Reports* 15 (2025), 39388. https://www.nature.com/articles/s41598-025-27053-2.

[13] Nothing in brain science is as simple as a "pleasure chemical". As the neuropsychologist Vaughan Bell observed, "Traumatised war veterans, for example, show nucleus accumbens dopamine surges when they are reminded of the sounds of battle, something they find deeply aversive." See https://www.theguardian.com/science/2013/feb/03/dopamine-the-unsexy-truth.

SB-2761-HD-2
Submitted on: 3/31/2026 12:02:32 PM
Testimony for JHA on 4/1/2026 2:00:00 PM

Submitted By	Organization	Testifier Position	Testify
Michael Olderr	Individual	Support	Written Testimony Only

Comments:

This bill seems like a security overreach. It's true that children shouldn't be exposed to social media, but the way this bill goes about it seems dystopian.

TECHNET
THE VOICE OF AMERICAN INNOVATION

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

March 31, 2026

Representative David A. Tarnas
Chair, Committee on Judiciary & Hawaiian Affairs
Hawaii State Capitol
415 South Beretania Street, Room 325
Honolulu, HI 96813

RE: SB 2761_SD2 HD2 (Keohokalole) – Relating to Social Media **- Oppose**

Dear Chair Tarnas, and members of the committees,

On behalf of TechNet, we respectfully oppose SB 2761 SD2 HD2. While TechNet supports efforts to ensure the safety and well-being of children online, we must respectfully oppose the bill due to its requirements to institute age verification and parental consent requirements that are in tension with consumer privacy and constitutional rights.

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 more than 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 appreciate the intent of this bill and share the commitment to providing a safe and secure online experience for children. TechNet members strongly believe that children deserve a heightened level of security and privacy online, and the industry is actively working to incorporate protective design features into apps, websites, and platforms. For example, some platforms allow minors to set reminders to take breaks or establish settings that protect them from potential threats or unwanted contact. TechNet members are also including parents and guardians in their child's experiences via parental supervision tools. We believe that empowering parents and guardians and their children to have an informed dialogue about navigating the internet and social media, accompanied with providing them with necessary safety and security tools and features, is a strong approach to children's online wellbeing.

<u>Age Verification</u>

SB 2761 SD2 HD2 requires app store providers to verify the age of users before granting access to app downloads, purchases, or usage, regardless of the nature of

the app the user seeks to access. Age verification is a complex challenge to address and requires consideration of how to properly balance the interests of privacy and security. Stringent age verification measures could necessitate the collection, processing, and storage of sensitive personal information, such as birth dates and government-issued identification. This could conflict with data privacy principles like privacy-by-design and data minimization and create new vectors for fraud, as every user in the state must prove whether or not they are a minor.

Parental Consent and Controls

Additionally, there are privacy concerns associated with the bill's parental consent requirements. Parental consent entails verifying parental relationships and parental rights, which will likely lead to privacy-invasive processes beyond collecting and verifying the age of an individual. For example, even with a birth certificate, there are custody agreements and other issues that could prevent a caregiver listed on that certificate from exercising parental rights to provide consent.

Constitutionality

We believe that there are likely constitutional issues with the bill that are similar to those identified by courts with other age verification and parental consent bills. A number of other states that have passed legislation with age verification requirements have had those laws challenged and enjoined due to constitutional concerns. Ohio's *Social Media Parental Notification Act* and Texas' SB 2420 are recent examples where courts have enjoined the laws from going into effect due to constitutional deficiencies.

In the case of Texas' SB 2420, which hews closely to SB 2761 SD2 HD2, a federal court found that the law was a content-based restriction on speech that failed strict scrutiny under the First Amendment. The court concluded that SB 2420 "is akin to a law that would require every bookstore to verify the age of every customer at the door, and for minors, require parental consent before the child or teen could enter and again when they try to purchase a book."[1] SB 2761 SD2 HD2 would likely suffer the same fate.

Enforcement

SB 2761 SD2 HD2 empowers the Attorney General to enforce compliance and allows parents to file civil lawsuits against those who fail to meet the bill's requirements. These provisions create significant legal and financial risks, particularly for smaller developers who may be less equipped to handle litigation.

[1] *Order Granting Motion for Preliminary Injunction*, CCIA v. Paxton, No. 1:25-cv-01660 (W.D. Tex. Dec. 23, 2025) (Pitman, J.).

TECHNET
THE VOICE OF AMERICAN INNOVATION

The cumulative impact of new legal obligations, uncertainty in how to comply, and the potential for litigation threatens to stifle innovation.

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

SB-2761-HD-2
Submitted on: 4/1/2026 11:07:28 AM
Testimony for JHA on 4/1/2026 2:00:00 PM

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.

SB-2761-HD-2
Submitted on: 4/1/2026 12:16:12 PM
Testimony for JHA on 4/1/2026 2:00:00 PM

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

Comments:

Aloha Chair and Members of the Committee,

I am a Hawai‘i resident with younger siblings who regularly use gaming apps like Roblox. While I understand and support the goal of SB2761 to protect our keiki online, I respectfully oppose expanding the bill to include all apps, especially gaming platforms. From what I've seen, gaming apps serve a different purpose than social media—they are spaces for creativity, collaboration, and entertainment, not primarily social networking.

My siblings use these platforms to play with friends, build games, and express creativity. Many of these apps already have safety features like chat filters, reporting systems, and parental controls. Expanding regulations without clearly distinguishing between types of platforms could unintentionally limit access to these positive experiences and place unnecessary restrictions on how young people engage online.

Rather than broadening SB2761 to cover all apps, I encourage a more targeted approach that focuses specifically on platforms designed for social interaction. Strengthening education, awareness, and existing safety tools may be a more effective way to protect youth without overregulating spaces that provide real benefits. Mahalo for the opportunity to share this testimony.