June 26, 2026

Attorney General's Office
California Department of Justice
Elihu Harris Auditorium
1515 Clay Street
Oakland, CA 94612

Re: California Department of Justice to Solicit Public Comment on SB 976, the "Protecting Our Kids from Social Media Addiction Act," as Part of Preliminary Rulemaking Process

Dear Attorney General Bonta:

On behalf of the Computer & Communication Industry Association ("CCIA"),[1] I write in response to the California Office of the Attorney General's ("California OAG's") solicitation of public comment to inform its upcoming rulemaking on SB 976, the "Protecting Our Kids from Social Media Addiction Act" (Cal. Health & Safety Code Sec. 27000 *et seq.*) ("POKSMAA").[2]

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.[3] 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.

These comments provide some key considerations to ensure effective and balanced approaches to protecting online safety and privacy. As CCIA and other organizations have noted,[4] California OAG should avoid restrictive regulations that would effectively force online services to institute age verification to ensure compliance. Instead, the California OAG should promote online safety through voluntary measures that do not jeopardize users' sensitive personal information.

---

[1] CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For 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] *Available at* https://oag.ca.gov/news/press-releases/california-department-justice-solicit-public-comment-sb-976-protecting-our-kids.

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

[4] Letter from TechNet, CCIA, et al., to The Hon. Anna M. Caballero, Chair, Senate Appropriations Committee, Re: SB 976 (May 6, 2024), https://ccianet.org/wp-content/uploads/2024/05/TechNet-Led-Coalition-Letter-CA-SB-976-Oppose.pdf.

Clear definitions are essential to avoid negative implications for California users and businesses.

Regulatory certainty is crucial in giving technologists and entrepreneurs the means to thrive and innovate. Ambiguous or sweeping definitions in proposed rules or regulations could capture services beyond the lawmakers' intent, and penalize products that curate content. Overly broad definitions are likely to discourage lawful design that benefits users of various digital services, including local small businesses.

Additionally, internet users often move between online services and should be able to rely on clear, consistent protection across the internet. The OAG should therefore avoid rules that unnecessarily subject different websites to different requirements.

Because of age verification's constitutional problems, the OAG should hold covered operators to an actual knowledge standard.

Beginning in 2027, Section 27001(a) of POKSMAA requires that covered operators must not provide an "addictive feed" to a user unless "the operator has reasonably determined that the user is not a minor" under the Attorney General's guidelines, or "has obtained verifiable parental consent." If the OAG holds covered operators to a standard beyond actual knowledge, it becomes virtually impossible for operators to determine when they are complying with the law. Consequently, unless operators are held to the actual knowledge standard in Section 27001(a)(1), they will effectively be forced to adopt age verification or parental consent requirements to ensure compliance.

Effectively forcing online services to adopt such requirements raises serious constitutional concerns. Several federal courts have held that laws requiring age verification and parental consent for social media sites violate the First Amendment's guarantee of free speech. The Supreme Court has repeatedly ruled that the First Amendment applies to teens as well as adults, holding that "[m]inors are entitled to a significant measure of First Amendment protection, and only in relatively narrow and well-defined circumstances may government bar public dissemination of protected materials to them."[5] The Court has further held that "to foreclose access to social media altogether is to prevent the user from engaging in the legitimate exercise of First Amendment rights."[6] Forcing covered operators to adopt age verification contradicts this ruling, foreclosing a wide range of protected speech for a population clearly entitled to access it. Such laws, in the Court's words, "do not enforce parental authority over children's speech . . . ; they impose *governmental* authority, subject only to a parental veto."[7] For these reasons, a wide array of lower courts have held that the First Amendment does not permit states to require age verification or parental consent to access protected speech as well.[8]

---

[5] *See, e.g.*, *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 212-13 (1975); *Brown v. Ent. Merchs. Ass'n*, 564 U.S. 786, 794 (2011).
[6] *Packingham v. North Carolina*, 582 U.S. 98, 108 (2017).
[7] *Brown*, 564 U.S. at 795 n. 3.
[8] *See, e.g.*, *NetChoice v. Jones*, 822 F. Supp. 3d 656 (E.D. Va. 2026); *NetChoice v. Murrill*, 812 F. Supp. 3d 594 (M.D. La. 2025); *NetChoice v. Carr*, 789 F. Supp. 3d 1200 (N.D. Ga. 2025); *NetChoice v. Griffin*, No. 23-cv-05105, 2025 WL 978607 (W.D. Ark. Mar. 31, 2025); *SEAT v. Paxton*, 765 F. Supp. 3d 575 (W.D. Tex. 2025); *NetChoice v. Reyes*, 748 F. Supp. 3d 1105 (D. Utah 2024); *CCIA v. Paxton*, 747 F. Supp. 3d 1011 (W.D. Tex. 2024).

Implementing a statewide mandate with similar consequences in California would cause similar constitutional problems. To avoid these problems, the OAG should continue to hold covered operators to the actual knowledge standard in Section 27001(a)(1) in 2027 and beyond.

An age verification mandate would curtail individuals' ability to tailor their content preferences.

Besides its constitutional problems, age verification carries many negative policy consequences. Many products, both digital and physical, can have effective child safety features installed on them even if they are primarily designed for adults. For example, bicycles are designed for general use by adults, with standard frames and safety features like reflectors and brakes. However, parents can choose to add training wheels, smaller seats, or handlebar attachments to make the bicycle safer and more suitable for a child. Likewise, many devices and services have content filtering technologies that allow parents to individually tailor settings and preferences to select age-appropriate content for themselves and their children. These types of filters and settings, however, are not activated by default.

In addition to ensuring age-appropriate experiences, the ability to curate and personalize feeds lets all users explore their interests and form communities. Restrictive regulations of personalized feeds and algorithmic rankings impedes digital services' ability to provide their users with the relevant content they expect to receive.

Age verification mandates undermine privacy and security.

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.[9] 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.[10] Such dangers are far from hypothetical: several of the most devastating data breaches in recent years are directly attributable to age verification requirements.[11] Government officials could also access this sensitive data through enforcement inquiries.

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

[9] *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/.

[10] 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/.

[11] 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.

security.[12] For these reasons, a group of 438 privacy and data security scientists has recently urged policymakers to institute a moratorium on age verification requirements until better solutions emerge.[13] Though the intention to keep kids safe online is commendable, this bill undermines that initiative by requiring more data collection about young people.

CCIA believes that targeted protections, including parental controls, filtering tools, and media literacy education, offer greater safety than age verification mandates. By working with businesses to continue their ongoing private efforts to implement safety and security mechanisms, the state can provide greater flexibility for families and service providers alike, and better safeguard free speech and privacy.

Age verification requirements undermine competition.

Collecting sensitive data from users, proactively screening it, and properly securing it is a cost-intensive barrier to entry for smaller businesses.[14] ID requirements also deter customers and can cut businesses' conversion rates by half.[15] Furthermore, as noted above, age verification provides targets for hackers. Startups are especially financially vulnerable to data breaches, which in 2025 cost companies an average of $160 per record, or $4.44 million per breach, enough to bankrupt many small companies.[16] Consequently, over 60 percent of startups close after being hacked.[17] For these reasons, 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 verify user ages.[18]

Current age determination tools estimate users' ages imperfectly.

There is no perfect method of age determination, and the more data a method collects, the greater risk it poses to consumer privacy[19] and small business sustainability.[20] A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, contains more information regarding guiding principles for age assurance and how digital

---

[12] *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.
[13] Joint Statement of Security and Privacy Scientists and researchers on Age Assurance (Mar. 9, 2026), https://csa-scientist-open-letter.org/ageverif-Feb2026.
[14] *See, e.g.*, Jesse Lieberfeld, *Knowledge Standards in Online Safety and Privacy Legislation*, CCIA (Apr. 14, 2026), https://ccianet.org/articles/knowledge-standards-in-online-safety-and-privacy-legislation/.
[15] *More Than Just a Number: How Determining User Age Impacts Startups*, Engine, 6 (Aug. 2024), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/66ad1ff867b7114cc6f16b00/1722621944736/More+Than+Just+A+Number+-+Updated+August+2024.pdf.
[16] *Cost of a Data Breach Report*, IBM (2025), https://www.ibm.com/reports/data-breach.
[17] Robert Johnson III, *60 Percent Of Small Companies Close Within 6 Months Of Being Hacked*, Cybercrime (Jan. 19, 2023), https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/.
[18] *Age Assurance: Guiding Principles and Best Practices*, Dig. Tr. & Safety P'ship, 10 (Sept. 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.
[19] Kate Ruane, *CDT Files Brief in* NetChoice v. Bonta *Highlighting Age Verification Technology Risks* (Feb. 10, 2025), https://cdt.org/insights/cdt-files-brief-in-netchoice-v-bonta-highlighting-age-verification-technology-risks/.
[20] Engine, *More Than Just a Number: How Determining User Age Impacts Startups* (Feb. 2024), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/66ad1ff867b7114cc6f16b00/1722621944736/More+Than+Just+A+Number+-+Updated+August+2024.pdf.

services have used such principles to develop best practices.[21] The report found that "smaller companies may not be able to sustain their business" if forced to implement costly age verification or assurance methods, and that "[h]ighly accurate age assurance methods may depend on collection of new personal data such as facial imagery or government-issued ID."[22]

Additionally, age estimation software will sometimes classify adults as minors, or vice versa, and does not process all populations with equal accuracy. The National Institute of Standards and Technology (NIST) recently published a report evaluating six software-based age estimation and age verification tools that estimate a person's age based on the physical characteristics evident in a photo of their face.[23] The report notes that facial age estimation accuracy is strongly influenced by algorithm, sex, image quality, region-of-birth, age itself, and interactions between those factors, with false positive rates varying across demographics, generally being higher in women compared to men. CCIA encourages lawmakers to consider the current technological limitations in providing reliably accurate age estimation tools across all demographic groups.

Even in proposals that do not explicitly mandate age verification, businesses often need to *determine the age of all users* to ensure that they can adhere to the regulations regarding minors. As explained above, this in turn requires using invasive age verification methods that force businesses to collect sensitive personal identifying information about their users.[24]

The age assurance reporting requirements undermine privacy protections.

Section 561(c) requires that covered operators publish detailed specifications on their websites regarding their age assurance methods and their success rates. However, publicizing these methods may give malicious actors a roadmap for undermining such systems' security. To avoid this problem, CCIA recommends instead requiring covered operators to keep written documentation of the listed specifications and provide them to the OAG upon request, and that the OAG must maintain the confidentiality of any reports received this way unless otherwise required by law.

The proposed rules incentivize aggregation of data which may undermine privacy.

Section 563(a)(8) states that "all information about the user known to the operator," without limitation, will be used in evaluating whether an age determination is "unreasonable." Similarly, Section 566 requires that "An operator with actual knowledge that a user is a minor or that reasonably determines that a

[21] *Age Assurance: Guiding Principles and Best Practices*, DTSP (Sept. 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.
[22] *Id.* at 10.
[23] Kayee Hanaoka et al., *Face Analysis Technology Evaluation: Age Estimation and Verification (NIST IR 8525),* Nat'l Inst. Standards & Tech. (May 30, 2024), https://doi.org/10.6028/NIST.IR.8525.
[24] Berin Szóka, *Comments of TechFreedom In the Matter of Children's Online Privacy Protection Rule Proposed Parental Consent Method; Application of the ESRB Group for Approval of Parental Consent Method*, TechFreedom (Aug. 21, 2023), https://techfreedom.org/wp-content/uploads/2023/08/Childrens-Online-Privacy-Protection-Rule-Proposed-Parental-Consent-Method.pdf.

user is a minor must use this information across all points of access to the operator's platform." To fulfill these requirements, covered operators must aggregate a wide range of user data from different sources. Operators often deliberately isolate different types of user data as a privacy or cybersecurity preserving measure, and this requirement undermines those efforts. Furthermore, this requirement takes away operators' ability to set aside age signals that may be less reliable– a user may view a selection of content most often viewed by users in a particular age range, but using such evidence for compliance purposes would likely result in many inaccuracies. To avoid these problems, CCIA recommends removing Section 563(a)(8) and clarifying that the consistent age determination requirement in Section 566 applies only when a user accesses the same account from different points and not when a user accesses the same service via different accounts. These changes will help ensure that user data is not collected or aggregated unnecessarily.

Terms such as "addiction" or "addictive" in an online context lack an adequate scientific foundation.

Humans engage in various compulsive and repetitive behaviors — some of which may negatively impact physical and/or mental health. Compulsive behaviors could range from binge eating unhealthy foods to exercising excessively to watching favorite shows for hours on end. However, certain regular activities do not necessarily amount to "addictions". The most recent edition of the *Diagnostic and Statistical Manual of Mental Disorders: Fifth Edition Text Revision (DSM-5-TR)* declined to include definitions for "Internet gaming disorder," "Internet addiction," "excessive use of the Internet," or "excessive use of social media," noting that "[g]ambling disorder is currently the only non-substance-related disorder included in the *DSM-5-TR* chapter 'Substance-Related and Addictive Disorders.'"[25]

The connected nature of social media has led to allegations that online services are negatively impacting teenagers' mental health. Researchers argue that existing evidence does not adequately support this theory and often mirrors the "moral panic" associated with new technologies. Studies from leading universities indicate that depression has virtually no causal relation to social media use.[26] Even the often-cited U.S. Surgeon General Advisory *Social Media and Youth Mental Health* discusses both potential risks and benefits of social media use among children and adolescents. It concludes, for example, that social media connects young people with communities who share their identities, abilities, and interests.[27] It can also provide access to important information and create spaces for self-expression. Social media can especially benefit at-risk youth, as online peer support can mitigate the stresses they face.[28]

---

[25] Am. Psychiatric Ass'n, *Diagnostic and Statistical Manual of Mental Disorders: Fifth Edition Text Revision* (2022).
[26] Amy Orben et al., *Social Media's Enduring Effect on Adolescent Life Satisfaction*, PNAS (May 6, 2019), https://www.pnas.org/doi/10.1073/pnas.1902058116.
[27] Off. of the Surgeon Gen., U.S. Dep't of Health & Human Servs., *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory*, *Social Media Has Both Positive and Negative Impacts on Children and Adolescents* (2023), https://www.ncbi.nlm.nih.gov/books/NBK594763/.
[28] *Id.*; *see also* Jennifer Marino et al., *Social Media Use and Health and Well-being of Lesbian, Gay, Bisexual, Transgender, and Queer Youth: Systematic Review*, J. Med. Internet Rsch. (Sept. 22, 2021), https://www.jmir.org/2022/9/e38449.

Without any medical consensus on the topic, private businesses cannot be expected to make coherent or consistent diagnostic assessments of what might constitute "addiction." A simpler and clearer approach would be to specify what types of data businesses may process under what circumstances, rather than attempting to relate such rules to an indefinite concept.

The OAG should forego enforcement of time-based notification restrictions while litigation is pending.

In *NetChoice v. Bonta*, the U.S. District Court for the Northern District of California preliminarily enjoined several provisions of SB 976, including the proposed restriction on nighttime notifications. The District Court held that such prohibitions "restrict significant amounts of speech for little gain", and thus likely violated the First Amendment.[29] However, per Section 551(c)(2), the proposed rules would enforce the enjoined nighttime notification requirements. CCIA therefore requests that the proposed rules stipulate that the nighttime notification requirements not be enforced until the litigation challenging these requirements has been resolved.

The OAG should clarify what measures operators must take to prevent location concealment.

Section 565 requires operators to institute anti-circumvention measures, and to consider "how a user can conceal or misrepresent whether they are located in the State of California," including "any data regarding the geographic location of a user that is collected for other purposes, including marketing, commercialization of user engagement, or generating personalized content." Without further clarification, this measure may force operators to further undermine user privacy to ensure compliance, such as by instituting location-based tracking of users. CCIA therefore recommends clarifying that any reliable industry standard anti-circumvention measures will be deemed sufficient for compliance with this section.

The required reports regarding indicators of users' ages are susceptible to misuse.

Section 567 requires operators to investigate in good faith and respond to all reports that a user is a minor. This rule requires modification to ensure that operators need not respond to spam requests, or to requests intended solely to silence other users. CCIA recommends that this requirement apply only when parents or guardians submit evidence to establish their right to supervise another user's account. Doing so would limit potential misuse of this requirement.

The data use limitation contradicts the limitation in the cited statute.

Section 561(e)(2) regulates operators' use of data collected for age assurance purposes, providing that "Data collected for the purpose of complying with this section... Must not be used for any purpose other than to comply with this section", citing Section 27001 of the California Health and Safety Code. However, the California Health and Safety Code allows

[29] *NetChoice v. Bonta*, 761 F. Supp. 3d 1202, 1227 (N.D. Cal. 2024).

operators to retain age assurance data for "compliance with this chapter or with another applicable law."[30] CCIA recommends conforming the proposed rules to the underlying statute and allowing the retention of age assurance data for compliance with any applicable law. Doing so avoids situations where covered operators must obtain age assurance data to comply with multiple laws, each of which prohibits use of the data for compliance with the others.

* * * * *

We appreciate your consideration of these comments. CCIA looks forward to continuing to participate in the ongoing regulatory process, including reviewing and providing feedback on any proposed rules or regulations. We hope you will consider CCIA a resource as these discussions progress.

Sincerely,

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

[30] Cal. Health & Safety Code § 27001(b) (West 2024), https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=HSC&sectionNum=27001.