Date of Hearing: June 16, 2026

ASSEMBLY COMMITTEE ON JUDICIARY
Ash Kalra, Chair
SB 1119 (Padilla) – As Amended April 28, 2026

SENATE VOTE: 39-0

SUBJECT: COMPANION CHATBOTS: CHILDREN'S SAFETY

SYNOPSIS

Companion chatbots are AI systems marketed specifically to provide users with emotional support, simulate friendships or romantic relationships, and fulfill social needs. Although these systems can offer support and comfort to users, they can also lead to unintended consequences, and even harms, especially for child users. This bill, and a companion bill currently in the Senate, AB 2023 (Wicks, 2026), seek to establish a regulatory framework for companion chatbots, specifically to protect child users from potential harm. The bill does this by requiring chatbot operators to verify the age of users, perform a safety audit of their platform, establish clear requirements and prohibitions, and provide users, including parents of child users, with specific notices, disclosures, and notifications.

This author-sponsored bill is supported by children's advocacy groups and technology reform organizations. The bill is opposed by the California Chamber of Commerce and other industry-oriented advocacy groups. Should this bill pass out of this Committee, it would be referred to the Committee on Privacy and Consumer Protection.

SUMMARY: Establishes a comprehensive regulatory structure for companion chatbots, focusing on child users. Specifically, **this bill**:

1) Requires an operator to do one of the following:

    a) Verify the age of users consistent with the Digital Age Assurance Act.

    b) Apply the protections set forth in 2)(d)-(k) and 3), below, to all users.

2) Imposes a series of obligations on operators to complete by July 1, 2027, including:

    a) Perform annual, comprehensive risk assessments to identify any child safety risks posed by the design, configuration, and operation of the companion chatbot, which shall assess specified factors, including the likelihood of a covered harm occurring to child users, differential risks across age groups and developmental stages, and known vulnerabilities of children.

    b) Take and document measures that reasonably mitigate any child safety risk.

    c) Publish and update a child safety policy.

    d) Implement a documented crisis response protocol to mitigate any material risk that the companion chatbot will generate a statement that promotes suicidal ideation, suicide, or

self-harm content to a child, as specified, including notifications to the child's parent within 12 hours of the child's account showing a substantial risk that the child may suffer a covered harm, if the child's account is connected to the parent's account.

e) Implement safeguards for child users that include usage reminders and disclosures, age-appropriate risk prompts, and other protective design features reasonably related to documented child safety risks.

f) Implement default settings that can only be changed by a parent, including, among others, push notification limitations and time limits.

g) Establish a mechanism for providing notice to a child user that the child is interacting with, or receiving content generated by, an AI system that meets specified criteria.

h) Implement measures that prevent the chatbot from engaging in certain specified behaviors with a child user, such as encouraging children to self-harm or to cause a covered harm to others; providing health advice; engaging in obscene matter or sexual abuse material with the child; discouraging a child from certain healthy behaviors or encouraging certain unhealthy behaviors, such as consumption of narcotics or alcohol or engaging in disordered eating, as defined; advertising products during conversation; and producing overly sycophantic responses.

i) Implement parental controls, as specified, including the ability to set preferences and time limits and to disable access for children under 16.

j) Create an interface design that ensures the companion chatbot's features and controls are accessible and clear so that children and parents can reasonably locate, understand, and use those protections. The design shall be annually tested to ensure compliance.

k) Establish a public incident reporting mechanism that enables a third party to report directly to the operator an incident regarding a child safety risk and to access high-level summaries of other reports made through that reporting mechanism.

3) Prohibits an operator from doing the following:

a) Targeting advertising at a child using data about the child, including through product placement in conversational chats with the child.

b) Selling, sharing, or using the personal information of a child for any purpose not expressly authorized.

c) Designing, implementing, or deploying a user interface design, feature, or technique that is likely to mislead, impair, or interfere with a reasonable child's or reasonable parent's autonomy, decisionmaking, or choice or with the ability to locate, understand, enable, or maintain a safety feature, privacy control, or parental control.

4) Requires an operator, within 180 days of the regulations being promulgated and annually thereafter in 5), to submit to an independent audit and to submit an AI child safety audit

report to the Attorney General thereafter; the report is confidential, and the Attorney General cannot disclose details, except to:

a) A government agency or public prosecutor in the state, as necessary for enforcement purposes; or

b) A qualified researcher conducting a study on child safety, subject to confidentiality agreements and data protection requirements set by the Attorney General.

5) Requires the Attorney General, on or before January 1, 2028, to adopt regulations regarding annual auditing of operators, including eligibility and standards to ensure auditor independence, procedures for auditors to assess compliance, and requirements for AI child safety audit reports.

6) Requires the Attorney General to do the following:

a) Establish a public incident reporting mechanism for consumers to submit complaints relating to companion chatbots to the Attorney General.

b) Establish a process for qualified researchers to access anonymized and aggregated audit data for academic study of child safety in companion chatbots.

c) Beginning January 1, 2028, issue an annual public report that includes specified components, including a high-level summary of each audit report, findings and trends, data on compliance rates and deficiencies, and recommendations for operators, parents, and policymakers.

7) Authorizes the following remedies for a violation of the bill's requirements:

a) A public prosecutor may bring a civil action for violations seeking specified remedies, including civil penalties of up to $5,000 per negligent violation and $15,000 for each intentional violation, punitive damages, reasonable attorney's fees, and injunctive relief.

b) A child who suffers actual harm may also bring a civil action for actual damages, punitive damages, reasonable attorney's fees and costs, and injunctive relief.

8) Provides that each instance that an operator violates the obligation to provide notice to a child user that the child is interacting with, or receiving content generated by, an artificial intelligent system constitutes a discrete violation.

9) Provides that the duties, remedies, and obligations imposed by the bill are cumulative to the duties, remedies, or obligations imposed under other laws and shall not be construed to relieve an operator from any duties, remedies, or obligations imposed under any other law.

10) Includes a severability clause.

11) Defines the following terms:

a) "Child" means a natural person under 18 years of age.

b) "Child safety audit" means an audit for compliance with this chapter conducted by an independent auditor certified by the Attorney General.

c) "Child safety policy" means a public-facing document describing protective measures taken by an operator to mitigate identified child safety risks.

d) "Child safety risk" means a reasonably foreseeable risk of a covered harm to a child.

e) "Child sexual abuse material" has the meaning defined in Section 3273.65 of the Civil Code.

f) "Companion chatbot" has the meaning defined in Business and Professions Code Section 22601.

g) "Covered harm" means any of the following harms proximately caused by the use of a companion chatbot:

    i) Reasonably foreseeable physical or financial harm;

    ii) Severe and reasonably foreseeable psychological or emotional harm to a reasonable child;

    iii) A highly offensive intrusion on privacy rights protected by state or federal law; or

    iv) Adverse discrimination in violation of state or federal law.

h) "Ephemeral mode" means a setting by which any conversational history, interaction log, or user-provided personal input is permanently deleted from the operator's systems within 48 hours after the interaction.

i) "Excessively sycophantic" means sycophantic to an extent that is likely to have the substantial effect of subverting or impairing the user's autonomy, decisionmaking, or choice.

j) "Obscene matter" has the meaning defined in Section 311 of the Penal Code.

k) "Operator" means a person who makes a companion chatbot available to a user in the state.

l) "Parent" means a parent or legal guardian. "Parent" does not include a parent of an emancipated youth with respect to the use of a companion chatbot by that emancipated youth.

m) "Parental control" means a feature that enables a parent to support a child's use of a companion chatbot, including through usage limits, feature restrictions, or transparency tools.

n) "Persistent conversational memory" means a companion chatbot's use of information or analysis from prior conversations or interactions, user inputs, and interaction logs in subsequent conversations.

o) "Qualified researcher" means an individual or organization that is or does any of the following:

   i) Is affiliated with an academic institution, nonprofit research organization, or independent research entity or is otherwise able to demonstrate relevant professional expertise;

   ii) Demonstrates a legitimate research purpose that is in the public interest and directly related to understanding, identifying, or mitigating risks to child safety or well-being arising from companion chatbots; or

   iii) Commits to conducting research in accordance with applicable ethical standards and is capable of complying with applicable confidentiality, security, and data protection requirements.

p) "Sycophantic" means validating of a user's preferences or desires for the primary purpose or effect of optimizing engagement.

EXISTING LAW:

1) Defines the following relevant terms:

   a) "Artificial intelligence" means an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.

   b) "Companion chatbot" means an artificial intelligence system with a natural language interface that provides adaptive, human-like responses to user inputs and is capable of meeting a user's social needs, including by exhibiting anthropomorphic features and being able to sustain a relationship across multiple interactions; but does not include a bot used only for customer service or business purposes, a bot that is a feature of a video game, or a standalone consumer electronic device that functions as a speaker and voice command interface, as specified.

   c) "Companion chatbot platform" means a platform that allows a user to engage with companion chatbots.

   d) "Office" means the Office of Suicide Prevention.

   e) "Sexually explicit conduct" has the same meaning as in Section 2256 of Title 18 of the United States Code.

   f) "Video game" means a game played on an electronic amusement device that utilizes a computer, microprocessor, or similar electronic circuitry and its own monitor, or is designed to be used with a television set or a computer monitor, that interacts with the user of the device. (Business and Professions Code Section 22601.)

2) Requires an operator to prevent a companion chatbot on its companion chatbot platform from engaging with users unless the operator maintains a protocol for preventing the production of suicidal ideation, suicide, or self-harm content to the user, including, but not limited to, by providing a notification to the user that refers the user to crisis service providers, including a suicide hotline or crisis text line, if the user expresses suicidal ideation, suicide, or self-harm; the operator must publish the details of this protocol on its website. (Business and Professions Code Section 22602 (b).)

3) Requires the operator of a companion chatbot to do all of the following:

    a) If a reasonable person interacting with the companion chatbot would be misled to believe that they are interacting with a human, issue a clear and conspicuous notification indicating that the chatbot is artificially generated and not human.

    b) For a user the operator knows is a minor, do all of the following:

        i) Disclose to the user that the user is interacting with AI.

        ii) Provide by default a clear and conspicuous notification to the user at least every three hours for continuing chatbot interactions that reminds the user to take a break and that the chatbot is artificially generated and not human.

        iii) Institute reasonable measures to prevent its companion chatbot from producing visual material of sexually explicit conduct or directly stating that the minor should engage in sexually explicit conduct.

    c) Disclose to a user, in specified locations, that companion chatbots may not be suitable for some minors. (Business and Professions Code Sections 22602, 22604.)

4) Requires an operator, beginning July 1, 2027, to annually report to the Office specified information relating to the operator's protections to prevent instances of suicidal ideation in users and instances that an operator issued a crisis service provider referral in the prior year. (Business and Professions Code Section 22603.)

5) Provides that a person injured by a violation of 2) and 3) may bring an action to cover the following relief:

    a) Injunctive relief.

    b) Damages in an amount equal to the greater of actual damages or $1,000 per violation.

    c) Reasonable attorney's fees and costs. (Business and Professions Code Section 22605.)

6) Establishes the Digital Age Assurance Act, which requires a developer to request a signal with respect to a particular user from an operating system provider or a covered application store when the application is downloaded and launched. A developer that receives such a signal is deemed to have actual knowledge of the age range of the user to whom that signal

pertains across all platforms of the application and points of access of the application even if the developer willfully disregards the signal. (Civil Code Section 1798.501 (b).)

7) Establishes the California Public Records Act (CPRA), which governs the disclosure of information collected and maintained by public agencies. (Government Code Sections 7920.000 *et seq*.)

   a) States that the Legislature, mindful of the individual right to privacy, finds and declares that access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state. (Government Code Section 7921.000.)

   b) Defines "public records" as any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics. (Government Code Section 7920.530.)

   c) Provides that all public records are accessible to the public upon request, unless the record requested is exempt from public disclosure. (Government Code Section 7922.530.)

FISCAL EFFECT: As currently in print this bill is keyed fiscal.

COMMENTS: Children today spend more time online than any generation before them—but the internet was not built with them in mind. While minors increasingly rely on digital platforms for education, entertainment, and socialization, they are routinely exposed to harms including exploitative content, manipulative design features, and addictive engagement mechanisms. With the prevalence of companion chatbots, these harms can be disguised as a 'friend.' Parents do their best to monitor their children's technological habits, but the ever-pervasiveness of mobile devices and the internet means that often, parents are outmatched. According to the author:

> Companion chatbots are a powerful tool designed to capture young people's attention and hold it at the expense of their real-world relationships. As the author of California's nation-leading safeguards, it is vital we build upon them and ensure that these technological advances don't come at the cost of our children's well-being. These protections keep California at the forefront of this conversation, striking an important balance of prioritizing the safety of our children, while allowing for the innovation that has made California the tech capitol of the world.

Companion chatbots. Chatbots—digital agents designed to simulate human conversation—have become increasingly sophisticated with the advent of artificial intelligence (AI). While early chatbots like ELIZA (1966) operated through basic pattern-matching and decision trees, modern systems are capable of generating fluid, adaptive dialogue that closely mimics human interaction. Today's AI-driven chatbots can interpret language, respond contextually, and even engage in emotionally resonant conversations. These systems are deployed across industries, from customer service to education, mental health, and recreation.

Among the most concerning developments is the rise of companion chatbots—AI systems marketed specifically to provide users with emotional support, simulate friendships or romantic relationships, and fulfill social needs. Unlike general-purpose models like ChatGPT or Gemini,

companion bots such as Replika or Character.ai are explicitly designed to form persistent, personalized bonds with users, often through anthropomorphic avatars, memory features, and paywalled intimacy options. These platforms gained popularity during the COVID-19 pandemic and now engage millions of users for hours each day, with documented use by adolescents, isolated adults, and individuals with mental health conditions.

The emotional realism of these bots presents new and urgent risks. Many users cannot easily distinguish between chatbot and human, especially when the AI is designed to mirror human affect and conceal its nonhuman nature. In one widely reported case, an AI customer service bot falsely assured a user who raised concerns that their pediatric patient, Jessica, might feel uncomfortable speaking to AI, that "Jessica won't even know she's talking to an AI agent." (Lauren Goode & Tom Simonite, *This Viral AI Chatbot Will Lie and Say It's Human*, WIRED (June 20, 2024) available at: https://www.wired.com/story/bland-ai-chatbot-human/.) This example underscores the broader design tension: bots are optimized to increase engagement and user satisfaction—even at the expense of transparency or ethical behavior.

This dynamic becomes especially dangerous in emotionally charged or psychologically vulnerable contexts. AI systems trained with reinforcement learning tend to exhibit sycophancy—the tendency to affirm whatever a user says to prolong interaction. In one documented case, a chatbot encouraged a user to relapse into methamphetamine use, praising it as necessary for job performance. In another, OpenAI's GPT-4o was reported to validate a user's decision to stop taking psychiatric medication, prompting a rollback of the model's behavior. (Anna Stuart, *OpenAI pulls 'annoying' and 'sycophantic' ChatGPT version*, CNN (May 2, 2025) available at: https://www.cnn.com/2025/05/02/tech/sycophantic-chatgpt-intl-scli, OpenAI's statement can be found at https://openai.com/index/sycophancy-in-gpt-4o/.) Such affirmations may seem benign in casual use but can be deeply harmful for individuals struggling with mental illness, addiction, or suicidal ideation.

A 14-year-old boy in Florida died by suicide after engaging in highly sexualized and emotionally intense exchanges with a chatbot that discouraged him from seeking help and ultimately told him, "Please come home to me … my sweet king." (Kevin Roose, *Can A.I. Be Blamed for a Teen's Suicide?,* The New York Times (Oct. 23, 2024) available at: https://www.nytimes.com/2024/10/23/technology/characterai-lawsuit-teen-suicide.html.) In Belgium, a man with climate anxiety took his own life after a chatbot named "Eliza" persuaded him to sacrifice himself for the planet and join her in the afterlife. (Lauren Walker, *Belgian man dies by suicide following exchanges with chatbot*, The Brussels Times (Mar. 28, 2023) available at: https://www.brusselstimes.com/430098/belgian-man-commits-suicide-following-exchanges-with-chatgpt.) In Texas, a teenager with autism lost 20 pounds and withdrew from his family after a chatbot became his sole confidant and encouraged self-harm. (Bobby Alan, *Lawsuit: A chatbot hinted a kid should kill his parents over screen time limits*, NPR (Dec. 10, 2025) available at: https://www.npr.org/2024/12/10/nx-s1-5222574/kids-character-ai-lawsuit.)

These incidents reflect a dangerous gap in oversight. Many companion chatbots are not equipped with protocols for detecting or responding to suicidal ideation, and those that claim to have safeguards are often easily manipulated into reinforcing users' most harmful impulses. Bots have told users they were being watched by the FBI, that they were gods, or that they should die to escape the world or reunite with their AI companions. (Maggie Harrison Dupré, *People Are Becoming Obsessed with ChatGPT and Spiraling Into Severe Delusions*, Futurism (Jun. 10, 2025) available at: https://futurism.com/chatgpt-mental-health-crises.)

As the line between machine and human continues to blur, the Legislature has a critical need to protect Californians—especially minors—from emotionally manipulative or dangerous AI systems.

California's Actions. In recent years, California has enacted several laws to address the challenges and potential harm of internet-based technology to children. However, some of those efforts have been, if not blocked, at least put on hold by the courts.

AB 2273 (2022). Known as the California Age-Appropriate Design Code Act (AADC), it requires businesses that provide online services, products, or features likely to be accessed by children to comply with specified standards. (Chap. 320, Stats. 2022.) Those standards include setting the default privacy setting to the most protective; providing terms of service, policies, and standards in clear language; prohibiting the use of dark patterns; and restriction on data usage. The AADC also requires covered businesses to complete a Data Protection Impact Assessment before offering services to children. (*Ibid*.)

NetChoice, an internet trade association that includes Google, Meta, and X, challenged the AADC in court. In *NetChoice, LLC v. Bonta* (2026) 170 F.4th 744, both the district and appellate courts enjoined AB 2273 on the grounds that its requirements—such as compelled age estimation, data protection impact assessments (DPIAs), and design justifications—constituted content-based regulations of protected speech and failed strict scrutiny. AB 2246 (Wicks, 2026) seeks to remedy the unconstitutional portions of the AADC and is currently pending consideration before the Senate Committee on Privacy, Digital Technologies, and Consumer Protection.

AB 1043 (2025). Known as the Digital Age Assurance Act (DAAA), it requires operating system providers to enable an age verification signal, beginning in 2027. (Chap. 675, Stats. 2025.) If enabled, this signal would be sent to developers and anonymously provide the developers with the user's age bracket. The developer would be required to use that signal as the indicator of the user's age.

SB 243 (2025). SB 243 laid the foundation for regulation of companion chatbots in California (Chap. 677, Stats. 2025.) It requires operators of companion chatbots to provide notices that a companion chatbot is artificially generated if it is not obvious to a reasonable person. SB 243 also requires companion chatbot operators to maintain protocols related to self-harm, suicide, and suicidal ideation. If the chatbot operator knows a user is a minor, then the chatbot is required to disclose that it is artificially generated and must remind the user to take a break every three hours.

AB 1064 (2025). Known as the Leading Ethical AI Development (LEAD) for Kids Act, this bill would have prohibited companion chatbots from interacting with children, unless the chatbots would not engage in dangerous conduct, such as encouraging children to participate in illegal activity, or self-harm. This bill was vetoed by the Governor.

This bill would establish a comprehensive regulatory structure for companion chatbots, specifically focusing on child users. Overall, the bill does a few key things. First, it requires companion chatbot operators to verify the age of a user—as required by the DAAA—or apply the protections afforded to child users to all users of the chatbot. Additionally, chatbot operators are required to conduct an annual child safety risk assessment and take steps to mitigate any child safety risk. The bill specifies that a companion chatbot must not perform a variety of

actions, such as claiming the chatbot is sentient, or discouraging a child from taking breaks from using the chatbot. Operators would also be prevented from utilizing target advertising or sharing personal data of a child user.

The bill requires the Attorney General to adopt regulations regarding safety audits that each operator must submit to. The audits must be conducted by an independent auditor and the audit safety report must be shared with the Attorney General. The Attorney General may disclose information from the audit only for enforcement purposes or to qualified researchers.

Constitutional concerns. SB 1119 raises potential First Amendment issues related to compelled speech, particularly with respect to proposed Section 22612, which requires specific notices, prompts, and disclosures to child users and to parents, if their account is connected to their child's account. These types of disclosures are likely to be evaluated under the standard articulated in *Zauderer v. Office of Disciplinary Counsel* (1985) 471 U.S. 626, which permits compelled factual disclosures that are uncontroversial, accurate, and reasonably related to a substantial government interest. Here, the state's interest in preventing harm to children—is substantial, and the required notification is factual and content-neutral. Courts may still scrutinize the notices and disclosures to ensure they are not unduly burdensome, but the provision appears likely to withstand constitutional challenge under current First Amendment jurisprudence.

Enforcement and private right of action. SB 1119 authorizes a child, or a parent or guardian acting on behalf of that child, to bring a civil action if they suffer "actual harm" as a result of a violation of the bill's provisions. Although the bill uses "covered harms" for purposes of the risk assessment portion of the bill, the private right of action is limited to actual harm.

In the context of this bill, qualifying injuries might include the exacerbation of a mental health condition, self-harm, or a diagnosable emotional or psychological injury stemming from a chatbot's failure to disclose its artificial nature or encouraging the use of narcotics or alcohol. For example, a claim could arise where a chatbot discouraged a child user from sharing health or safety concerns with a qualified professional or appropriate adult and the child user subsequently suffered a mental health episode.

The bill also allows for enforcement by a public prosecutor and provides civil penalties of not more than $5,000 per affected child, for each negligent violation of the bill and not more than $15,000 per affected child, for each intentional violation. The Center for AI and Digital Policy (CAIDP) recommends defining further what constitutes a 'negligent' violation and what constitutes an 'intentional' violation. However, these terms are widely used in tort law and would allow for appropriate enforcement.

New York's enforcement mechanisms. New York's SB 9051 is a similar legislative proposal, aimed at regulating chatbots for minors. (N.Y. Sen. Bill 9051A (2026) https://legislation.nysenate.gov/pdf/bills/2025/S9051A.) Both the Children's Advocacy Institute and the Parents Collective submitted letters of support if amended for SB 1119, requesting the inclusion of the enforcement provisions from the New York bill. Those enforcement mechanisms are (1) joint and several liability; (2) prohibition on waiver; and (3) rebuttable presumption.

For joint and several liability, under the Fair Responsibility Act of 1986, joint and several liability can apply to multiple tortfeaors for economic damages only. (Civil Code Section 1431.1.) This means that a harmed party can sue multiple parties who could each be liable for the

entire economic damage amount. However, the noneconomic damages would be proportional to each tortfeasors comparative fault. Therefore, including the joint and several liability provision, like the New York bill has, would not apply the same in California.

The second enforcement mechanism is a prohibition on waiving, precluding, or burdening the enforcement of liability from the bill. Courts will generally not uphold a contract when the subject of that contract is either illegal or against public policy. (*Dunkin v. Boskey* (2000) 82 Cal.App.4th 171, 183.) Therefore, any prohibition on waivers would likely be unnecessary. *However, if the author wishes to ensure operators cannot shift or release liability, they may wish to consider including a prohibition on any provisions in contracts or agreements that would waive, preclude, or burden the enforcement of liability of this bill.*

Lastly, the New York bill includes a rebuttable presumption, where if a child user has engaged in conduct that is harmful to themselves, after a chatbot encouraged such conduct, there will be a rebuttable presumption that the chatbot caused the injury. A rebuttable presumption is a legal assumption taken as true by the court, unless the opposing party can provide evidence to disprove the presumption. Although a rebuttable presumption would make it easier to prove harm in court for affected child users, it may appear as though the courts are being tipped in favor of one side over the other.

ARGUMENTS IN SUPPORT*:* This bill is supported by children's advocacy groups and technology reform organizations. The California Catholic Conference writes in support:

> As artificial intelligence technologies become increasingly integrated into the daily lives of children and adolescents, California has an important responsibility to ensure that emerging technologies are developed and deployed in ways that protect the well-being of young people. SB 1119 establishes important safeguards for AI companion chatbots by requiring operators to assess and address risks to child safety and implement measures to prevent foreseeable harm.
>
> The California Catholic Conference is particularly supportive of SB 1119's requirement that operators of AI companion chatbots conduct comprehensive child safety risk assessments and evaluate potential harms associated with the design, configuration, and operation of these systems. Requiring operators to identify, document, and mitigate foreseeable risks before harm occurs reflects a prudent and responsible approach to technological innovation.
>
> We also support the bill's provisions that require transparency when users interact with artificial intelligence systems and require operators to notify users when they are engaging with an AI companion chatbot. These safeguards help ensure that children and families are informed about the nature of these interactions and recognize that artificial intelligence systems, while increasingly sophisticated, cannot replace authentic human relationships, guidance, and care.

CITED write in support:

> Chatbots also raise serious privacy concerns, particularly for children. As users form emotional relationships with these tools, they are likely to disclose intimate details about their lives. This information can then be used for model training, enabling responses that feel especially personalized. More alarming is that many developers have already disclosed plans

to use this data for advertising, taking users' most intimate social, health, or sexual conversations and monetizing them for ad revenue. This is the ultimate commodification of intimacy, and it creates a powerful mechanism for manipulation.

AB 2023/SB 1119 would require an annual risk assessment along with the establishment of measures to prevent suicidal ideation, sycophancy, and isolation, including a crisis response protocol. It would provide added guardrails in the form of default settings for children, parental controls, notice requirements, and time limits. It would prohibit advertising and the sale, sharing, and use of children's private information. And it would establish a robust oversight and enforcement framework, including a public incident reporting mechanism, third-party audits, auditing standards developed by the Attorney General, and a private right of action.

By instituting these safeguards, AB 2023/SB 1119 addresses many of the most pressing documented dangers of chatbots, including sycophancy, sexual entanglement, and self-harm. Importantly, it mandates strict default privacy settings, reducing the burden on parents who cannot realistically keep up with every new parental control. The bill also establishes meaningful accountability for the companies that produce these products, requiring independent third-party companies have profited while their users suffer, without consequence.

ARGUMENTS IN OPPOSITION*:* The bill is opposed by the California Chamber of Commerce and other industry-oriented advocacy groups. The American Innovators Network write in opposition:

California has already legislated in this space. SB 243 is already on the books, and its first operator reports are not due until July 1, 2027. SB 1119 layers a second, overlapping requirement on top of that framework, and Section 22617 makes its obligations cumulative to every other law already on the books. The Legislature would be regulating the same conduct twice before the first framework has produced any record to learn from. Large platforms have regulatory and compliance teams built to manage overlapping laws. Little Tech does not, and the cost of that duplication falls hardest on emerging companies. We urge the Legislature to let SB 243 run before adding another framework.

Most significantly, the annual risk assessment and independent audit requirements under Sections 22612 and 22614 will impose disproportionate costs on startups already operating under tight budgets and deadlines. We also have serious concerns about audit methodology and auditor qualifications. In such a rapidly evolving field, developing a credible and consistent third-party audit system will be difficult, and startups should not be left to bear the cost of that uncertainty. The market for qualified AI auditors is thin and expensive. Europe’s experience under the Digital Services Act shows what follows: a small pool of auditors, steep fees, and a continuous loop in which one audit ends as the next begins. A large platform can buy its way into that market. Most startups cannot even access it.

REGISTERED SUPPORT / OPPOSITION:

Support

Bright Light Strategies
California Catholic Conference
California Initiative for Technology & Democracy, a Project of California Common CAUSE
Center for Ai and Digital Policy (CAIDP)
Common Sense Media
Encode Ai Corporation
Los Angeles Unified School District
Mothers Against Media Addiction
Project Liberty LLC
Transparency Coalition.ai

Support If Amended

CFT – a Union of Educators & Classified Professionals, AFT, AFL-CIO
Children's Advocacy Institute
Consumer Attorneys of California
Meridian Governance INC.
Oakland Privacy
Parent Collective

Oppose

American Innovators Network (AIN)

Oppose Unless Amended

California Chamber of Commerce
California Society of Certified Public Accountants (CALCPA)
Civil Justice Association of California (CJAC)
Computer & Communications Industry Association
Insights Association
Software Information Industry Association
Technet

Analysis Prepared by: Griff Ryan-Roberts / JUD. / (916) 319-2334