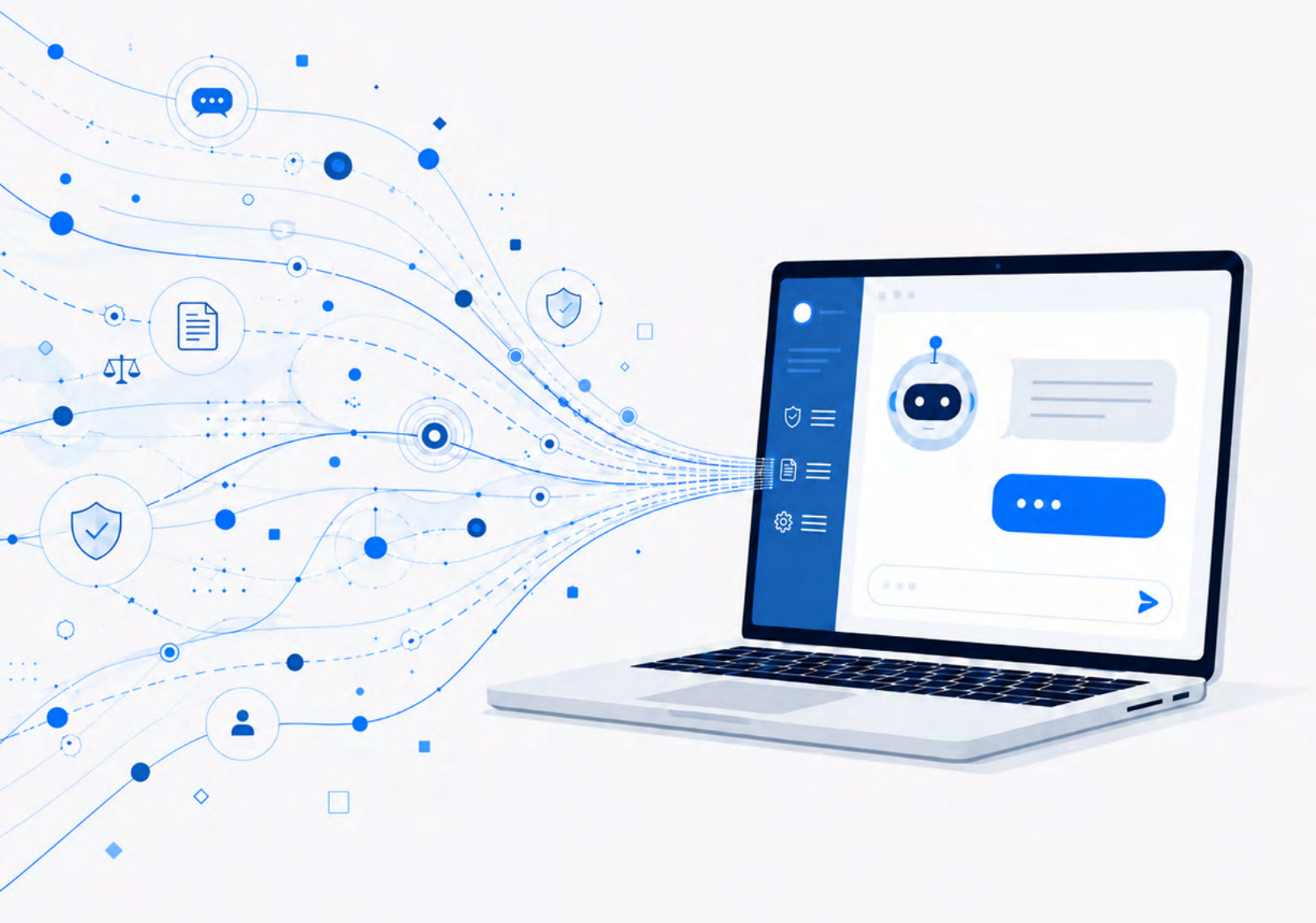
REGULATING THE CONVERSATION

The U.S. Landscape of AI Chatbot Legislation



FUTURE OF PRIVACY FORUM

AUTHOR

Justine Gluck
Policy Analyst, AI Policy and Legislation

EDITORS

Tatiana Rice, Senior Director for U.S. Legislation
Daniel Hales, Policy Counsel for U.S. Legislation
Matthew Reisman, VP for U.S. Policy

ACKNOWLEDGEMENTS

The author is especially grateful to Tatiana Rice for her editorial support throughout the report. The author would also like to thank Rafal Fryc (U.S. Legislation Intern) and Laken Rivet (U.S. Legislation Intern) for their research and citation support and Jordan Francis (Senior Policy Counsel) for his thoughtful feedback on the report.

The Future of Privacy Forum (FPF) is a global non-profit organization that advances principled and pragmatic data protection, AI and digital governance practices. We convene leaders across industry, academia, and the public sector to provide expert analysis, benchmarking, and best practices that support responsible innovation and regulatory compliance. Learn more about FPF by visiting fpf.org.

EXECUTIVE SUMMARY

In 2026, lawmakers across the country confronted a new dimension of AI regulation: how to govern systems that do not just generate content, but interact conversationally and, often, emotionally with people. That question has quickly translated into a wave of chatbot-specific legislation across states and in Congress. The Future of Privacy Forum's report, ***Regulating the Conversation: The U.S. Landscape of AI Chatbot Legislation***, analyzes this emerging U.S. legislative landscape for chatbot regulation, with a focus on state laws and key proposals from 2025 and 2026. The report identifies five key takeaways:

1. **Chatbot regulation has become one of the most active areas of U.S. AI policymaking.** In 2026, 37 states introduced 124 chatbot-related bills, 13 of which have been enacted, bringing the total number of state chatbot laws enacted in 2025 and 2026 to 18. Much of this activity focused on companion chatbots and youth safety. This momentum has been driven in part by high-profile litigation alleging chatbot-related harms and policymakers' desire to act more proactively on chatbots than they believe they did on social media.

2. **Chatbot laws are regulating the user experience of AI.** Newly enacted chatbot laws focus on regulating the conversation and interaction between a user and the technology, especially when chatbots involve human-like and emotional interactions. This emphasis differs from other AI laws that focus on regulating how an AI model is trained or tested, or even the earlier wave of chatbot legislation in 2025, which centered primarily on user disclosures.

3. **Though no single state model has emerged, there are common regulatory trends.** Many laws require chatbot operators to provide user disclosures, implement crisis response and safety protocols, and apply minor-specific safeguards. Common minor-specific safeguards include parental controls and measures to prevent certain content, conduct, and relational behavior, such as emotional dependence and engagement optimization. Some laws also limit how chatbot operators can provide services requiring professional licensure or subject to other regulation, or require operators to implement certain data protection measures.

4. **Chatbot laws raise difficult questions about how to define and operationalize emerging risks.** The report highlights some of the ambiguities and policy tradeoffs around concepts such as emotional dependence, crisis detection, parental controls, and sensitive conversational data. These issues often require balancing user safety with privacy, autonomy, beneficial use cases, and the practical challenges of applying broad statutory concepts to context dependent chatbot interactions.

5. **The next phase of chatbot regulation may be shaped by unresolved legal and policy questions.** Existing and proposed laws may face preemption debates as Congress considers federal regulation. Lawmakers may also expand their focus beyond minors and companion chatbots to address other vulnerable users or sensitive contexts, while chatbot laws may become an early model for regulating agentic AI systems.

Reader's Guide

This report is designed for readers approaching chatbot regulation from different perspectives.

Readers looking for a high-level overview should start with the *Executive Summary*, *Introduction*, *Part I: Why Chatbots Became a Legislative Focus*, and the opening chart in *Part II: Core Components of a Chatbot Law*. Together, these sections explore the acceleration of chatbot regulation and what the main components of a state chatbot law look like.

Policymakers and regulators drafting or evaluating chatbot legislation may find *Part II* most helpful. This section explains the policy dynamics driving chatbot regulation, as well as key drafting and implementation tradeoffs that appear across enacted and pending laws.

Chatbot operators and compliance teams should also focus on *Part II*. This section identifies how different models may be scoped into existing laws, as well as other compliance triggers and questions involving implementation.

Policy experts, researchers, and journalists may find *Part I*, *Part III: The Next Phase of Chatbot Regulation*, and the *Conclusion* most useful for understanding the forces driving chatbot regulation and the unresolved questions that may shape its future, including federal preemption, expansion beyond youth, and agentic AI.

Readers looking for bill-by-bill detail should consult the *Appendix* charts, which categorize enacted and pending state and federal chatbot proposals and common legislative approaches.

Methodology and Terminology Note

This report analyzes chatbot-related legislation introduced or enacted in 2025 and 2026 based on bills tracked by FPF through September 2026. For purposes of this report, "chatbot legislation" includes bills focused on companion chatbots or AI companions, conversational AI services, mental health chatbots, integrated AI companion features, as well as federal chatbot proposals. Although the majority of the laws and proposals discussed focus on companion chatbots, the report applies "chatbot legislation" as an umbrella term because lawmakers use different terminology and definitions across bills and because many of the core policy questions may apply beyond companion chatbots as legislation evolves in the future. Where a section discusses a narrower category, such as mental health chatbots or integrated chatbots, the report identifies that narrower scope.

TABLE OF CONTENTS

Introduction 4

State Chatbot Legislation 5

Part I: Why Chatbots Became a Legislative Focus 6

Part II: Core Components of a Chatbot Law 7

A. Scope and Definitions 10

B. Baseline Transparency and Safety Requirements 13

1. General User-Facing Disclosure 13
2. Other User Disclosures: Minor Suitability and Professional-Service Disclaimers 14
3. Crisis Response and Safety Protocols 14

C. Minor Users and Age-Based Safeguards 16

1. Identifying Minors: Age Assurance and Knowledge Standards 16
2. Minor-Specific Safeguards 18

D. Other Requirements 23

1. Professional Licensure and Regulated Services 23
2. Data Protection 24

E. Enforcement and Liability 25

Part III: The Next Phase of Chatbot Regulation 27

A. Federal Preemption and State Authority 27

B. Beyond Youth: Expanding the Regulatory Focus 28

C. From Chatbots to AI Agents 29

Conclusion 30

Appendix 31

Endnotes 43

INTRODUCTION

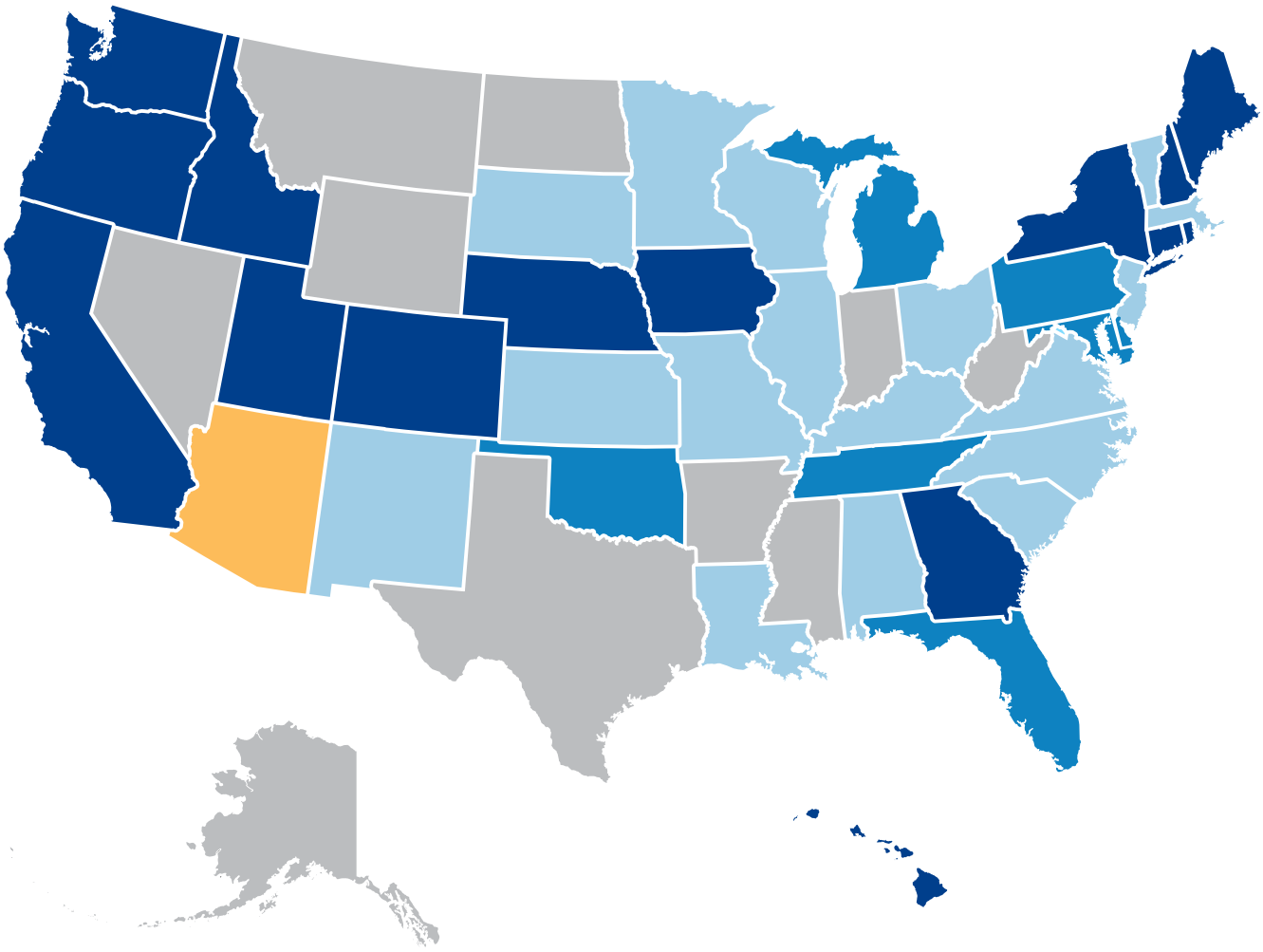
In a crowded year for AI legislation in the United States, chatbot regulation took center stage. Thirty-seven states introduced 124 chatbot-related bills in 2026, with thirteen of those signed into law–bringing the total number of state chatbot laws enacted in 2025 and 2026 to eighteen and making the topic one of the most active areas of AI policymaking.[1] That activity has also crossed party lines: 45 percent of bills were introduced by Republican lead sponsors and 55 percent by Democratic lead sponsors. The momentum is not surprising: chatbots sit at the intersection of many issues already dominating U.S. technology policy debates, including youth online safety, privacy, consumer protection, and mental health. But what sets chatbots apart from these familiar debates is the relational quality of the technology. Unlike a search engine or a social feed, a chatbot talks back, remembers context, and can create the powerful impression that it understands the user.

For many policymakers, the concern is not only that users interact with chatbots, but that some users, particularly young people, are beginning to rely on them for intellectual, emotional, and social needs.[2] That reliance can bring both benefits and risks: for some, chatbots offer access to AI tools and support that may not otherwise be available, while for others, they may fuel harmful behavior and actions with serious, sometimes fatal, consequences. Together, these concerns have pushed lawmakers across the political spectrum toward a common question: how should the law respond to AI systems that don't just generate content, but interact with humans directly?

Increasingly, lawmakers are answering that question by regulating the interaction itself, rather than the model underneath it. Because the chatbot is the most direct and visible way consumers encounter generative AI,[3] that user interface is where regulatory attention has concentrated. The user interaction is also where many online safety concerns arise: whether a chatbot reinforces harmful beliefs through sycophantic responses, becomes a substitute for human emotional support, or encourages prolonged use. Unlike other areas of AI regulation, such as frontier model regulation, which often focuses on how an AI model is developed and trained, chatbot laws generally ask a different set of questions, such as whether the chatbot identifies itself as non-human, how it responds when a user is in crisis, and whether users may mistake it for a licensed professional. In other words, lawmakers are often regulating the *conversation* chatbots have with users, not just the AI system powering it.

This report provides stakeholders with practical insight into this fast-evolving area of technology law and policy, including **(I) why chatbot legislation is emerging now; (II) the core components of chatbot laws and the policy tradeoffs they raise; and (III) the key questions that may shape the next phase of chatbot regulation.**

STATE CHATBOT LEGISLATION



LEGISLATIVE STATUS

- **None Introduced** — No chatbot-specific legislation identified during the period covered.
- **Introduced** — At least one qualifying bill was introduced.
- **Passed at Least One Chamber** — At least one bill passed a legislative chamber.
- **Enacted** — At least one bill was enacted.
- **Vetoed** — At least one bill passed the legislature but was vetoed by the governor.

PART I: WHY CHATBOTS BECAME A LEGISLATIVE FOCUS

Two forces are largely driving the current wave of chatbot legislation: high-profile litigation alleging chatbot-related harms and policymakers' desire to act more proactively on chatbots than they believe they did on other higher-risk services, particularly social media. Together, these forces have pushed lawmakers to focus on AI systems that can create sustained or emotionally responsive interactions with vulnerable users, especially minors.

In 2025, chatbot litigation became a major driver of public and legislative attention toward companion chatbot risks. Parents have brought a growing number of lawsuits after their children died by suicide or experienced serious self-harm following interactions with companion chatbots, while state attorneys general also brought consumer protection enforcement actions challenging chatbot safety practices.[4] In these cases, plaintiffs broadly allege[5] that inadequate or missing safeguards in chatbot systems contributed to serious injury or death, and many have since advocated for greater accountability and more proactive safety obligations.[6]

This litigation has helped focus chatbot legislation on minors, companion chatbots, and crisis response. The relationship between litigation and legislation appears mutually reinforcing: lawsuits are surfacing risks of harm and potential guardrail gaps in law and practice, while new laws are beginning to translate those risks into concrete duties that could mitigate harm and shape future litigation. For example, in *Garcia v. Character Technologies*, plaintiffs alleged that a minor died by suicide after developing a relationship-like attachment to a companion chatbot and that chatbot features designed to simulate human-like, emotionally dependent, and sexualized interactions contributed to the harm, along with alleged gaps in safeguards related to age, parental oversight, crisis intervention, warnings, and reporting.[7] Those allegations map closely onto emerging legislative requirements discussed in Part II and are highlighted in more detail in *Appendix Chart I*.

As litigation and enforcement activity expanded, chatbot safety debates also began to move beyond suicide prevention and self-harm. Florida's 2026 enforcement action against OpenAI, for example, alleged that ChatGPT facilitated violent planning, advice on illicit use of weapons, and other criminal conduct.[8] Around the same time, several state proposals began incorporating provisions related to harm to others, suggesting that chatbot safety obligations may increasingly extend to broader public-safety risks.[9]

But litigation is not the only force driving this activity. Policymakers also appear to be drawing on concerns from earlier technologies, such as the social media context—including the view that earlier regulatory intervention could have helped to address youth safety risks before they became more difficult to mitigate later.[10] Many regulators now largely view social media platforms as higher-risk services, demanding greater safety protections for minors to mitigate potential risks of harm. For instance, Senator Cantwell (D-WA) argued that Congress "failed to act" as social media became more widespread and harmful to children and that lawmakers should not "make the same mistake now that AI is becoming more pervasive."[11]

This social media analogy helps explain the urgency behind many chatbot bills and why several regulatory components of chatbot bills reflect requirements seen in other youth online safety laws, such as age assurance, parental controls, access restrictions, content restrictions, and restrictions on engagement optimization. Similar to social media platforms, lawmakers are quickly identifying services offering conversational chatbots as higher-risk products that owe more robust safety protections to users, especially minors, while still preserving the technology's potential benefits. However, even if there are common design elements and risks of harm, chatbots and social media platforms are different technologies—and those differences lend to distinct considerations of harm. In addition to similar concerns about minors' exposure to

illicit content or higher-impact design features observed in other higher-risk services,[12] chatbot laws also look to govern the unique interaction and relationship the system may *create* with a user.

This distinction may also suggest why lawmakers are considering chatbot-specific obligations, even though some existing consumer protection, data privacy, professional licensure, online safety, and tort laws already apply to chatbots, as the litigation illustrates. Parents, advocates, and lawmakers have increasingly argued that these generally applicable laws may be insufficient on their own because they often operate retrospectively, addressing harm after the fact rather than preventing it. Recent chatbot bills therefore seek to impose more proactive safeguards before harm occurs, rather than relying solely on after-the-fact remedies.

PART II: CORE COMPONENTS OF A CHATBOT LAW

These policy concerns have not produced a single legislative model, but they have produced significant legislative momentum, with many states enacting laws that converge around a recurring set of regulatory building blocks. The first wave of chatbot laws, enacted by five states in 2025, largely focused on non-human disclosures and crisis-resource referrals for users expressing suicidal ideation or self-harm.[13] In 2026, state activity accelerated and expanded beyond that baseline toward more substantive regulation of chatbot interactions and design. ***Appendix Chart II*** identifies state chatbot bills enacted or passed by the legislature in 2025 and 2026. While many states enacted chatbot-specific laws, chatbot regulation was also reflected in omnibus AI laws and mental health or professional licensure laws that regulate conversational AI systems. Among the 18 laws regulating chatbots enacted in 2025 and 2026, all of which were passed on the state level, most contain the following elements:

A. Scope: Most laws regulate operators of companion chatbot systems;

B. Requirements: Most laws require operators to provide user disclosures, implement a crisis response and safety protocol, and identify minors to set minor-specific safeguards. Some laws also limit how operators can provide chatbots in professionally licensed areas, like licensed behavioral or mental health services, or how they must maintain certain data protection measures.

C. Enforcement: Most laws are enforced by the state's Attorney General as a consumer protection violation. Some laws permit private rights of action by injured individuals.

However, each law varies significantly in its specific requirements. This section breaks down recurring components that appear across enacted laws while also flagging practical implementation questions and notable approaches in pending bills. Not every law contains every component: some include only a few core requirements, while others take a more comprehensive approach.

The key components, and a high-level overview of their respective trends and tradeoffs, are illustrated on the following pages.

Component	What It Determines	Emerging Pattern	Key Policy Considerations
Section A: Scope			
Scope and Definitions	Which chatbot systems are covered	States are using different definitional models, including capability-based definitions, behavior-based definitions, and broad definitions narrowed by significant carveouts	If laws aim to address risks associated with companion-like chatbot systems, how can they do so without sweeping in lower-risk tools, such as customer service, education, gaming, or productivity chatbots?
Section B: Baseline Transparency and Safety Requirements			
User Disclosures	Whether and how users are told they are interacting with AI	Disclosure is the baseline safeguard, but proposals increasingly add more frequent minor-specific notices and professional-service disclaimers	How can disclosures help users understand they are interacting with AI without creating disclosure fatigue for users?
Crisis Response and Safety Protocols	How chatbots detect and respond to user indications of self-harm, suicide, eating disorders, or other serious harms	Laws are moving from crisis hotline disclosures toward more robust safety protocols, reporting, and possible escalation	When risk for self-harm, suicidal ideation, or harm to others is detected, what response is appropriate, and how should user privacy be protected?
Section C: Minor Users and Age-Based Safeguards			
Age Assurance and Knowledge Standards	How operators identify minor users	Most enacted laws rely on knowledge standards, while other bills add targeted age assurance and default controls. Some laws are also requiring more robust parental tools	Should certain features and access be restricted for minors? If so, how should laws determine when a user is a minor without requiring unnecessary collection of sensitive age-related data? How can laws calibrate a proportionate knowledge standard to an identified risk? What, if any, barriers may be generated for non-minor users by incorporating these restrictions?

Component	What It Determines	Emerging Pattern	Key Policy Considerations
Section C: Minor Users and Age-Based Safeguards (continued)			
Parental Controls	Whether parents or guardians can manage minor users' access, account settings, privacy settings, or chatbot-specific features	Laws are moving from basic account and privacy tools toward more feature-specific controls, including limits on memory, personalization, relationship simulation, time spent, and access to certain companion chatbot features	Should parents or guardians be provided certain tools or controls over their child's use of a chatbot? If so, how can these tools/ controls protect minors without undermining teen privacy, autonomy, or access to beneficial uses? Should controls be offered, enabled by default, or required for certain high-risk features?
Content, Conduct, and Relational Restrictions	What chatbots may generate, depict, encourage, or facilitate for minor users, including sexually explicit content and interactions involving self-harm, violence, eating disorders, and other harmful conduct, as well as whether chatbot features or interaction patterns can encourage prolonged use, inappropriate emotional dependence, or relationship-like interactions.	Laws increasingly regulate not only potentially harmful content itself, but whether a chatbot affirmatively encourages or facilitates harmful conduct, as well as the cumulative relationship between a user and chatbot.	How can potentially harmful chatbot outputs or conduct be identified and addressed without discouraging safe or help-seeking conversations about sensitive topics? Should these mitigations be minor-specific or generally applicable to all users? Are there First Amendment implications to content restrictions? How can laws distinguish ordinary personalization or product engagement from design features that encourage unhealthy reliance or prolonged use? How should ambiguous concepts such as "inappropriate emotional dependence" be defined and operationalized?

Component	What It Determines	Emerging Pattern	Key Policy Considerations
Section D: Other Requirements			
Professional Licensure and Regulated Services	To what extent can a chatbot provide support services akin to those provided by regulated professionals?	Laws focus especially on restricting representations of licensed mental health professionals, but some extend to legal or other licensed services	Should there be limitations to a chatbot offering professional/ licensed advice, especially in the mental health sector? Where is the line between general information, emotional support, and regulated professional advice?
Data Protection	How chatbot conversations, memory, and age data may be used and shared	Data protection remains less common in enacted laws, but some proposals are starting to target advertising, model training, memory, and retention	How can laws protect sensitive conversational data that operators may need to collect and retain to implement chatbot safety requirements?
Section E: Enforcement and Liability			
Enforcement and Liability	Who can enforce the law and what remedies are available	Attorney General enforcement dominates, while private rights of action appear but are less common in enacted laws	How can laws ensure accountability for harms without introducing inappropriately broad or unpredictable litigation exposure?

A. SCOPE AND DEFINITIONS

While the scope of covered entities remains mostly consistent across chatbot laws, the scope of covered technologies remains a central challenge. Most state chatbot laws apply to chatbot "operators," largely defined as a person or entity that makes a chatbot available to the public or a user residing in the state. A few states, including Hawaii, Iowa, and Idaho, include an exemption for mobile application stores or search engines that solely or merely "provide access" to the chatbot. The more significant scoping questions tend to concern which *chatbot systems* are covered, rather than which user-facing entity bears the primary obligations.

For the scope of covered technologies, lawmakers are generally trying to regulate systems that create companion-like risks, such as sustained personal conversation or emotional responsiveness, without sweeping in systems used for limited purposes, such as ordinary customer service bots, research and education tools, gaming features, and productivity assistants. That boundary is difficult to draw because chatbot products are increasingly multi-use. A system may not be marketed as a companion chatbot, but it may still become companion-like through repeated interactions or emotionally responsive design. As a result, scope and definitions are doing much of the substantive work in state chatbot laws.

States are beginning to approach this scoping problem through three broad definitional models: capability-based definitions, behavior-based definitions, and broad definitions narrowed by carveouts.

Definitional Models for State Chatbot Laws

Definitional Model	Basic Approach	Examples	Why It Matters
Capability-Based Definitions	Focus on what a system is "capable" of doing, such as providing "adaptive, human-like responses" or "sustaining a relationship across multiple interactions."	California Washington Connecticut[14]	May capture systems even when companionship is not their primary purpose, because capability, rather than marketing or actual use, is the trigger.
Behavior-Based Definitions	Focus on how the system operates in practice, such as whether it "retains information on prior interactions" and user preferences, asks "unsolicited emotional-based questions," and "sustains an ongoing dialogue concerning matters personal to the user."	New York Oregon Rhode Island Georgia Hawaii	May be more targeted than capability-based definitions, but still raises questions when ordinary tools become more personalized or emotionally responsive over time.
Broad Definitions with Carveouts	Begin from a wider category of systems that "simulate human conversation," often paired with a long list of carveouts.	Idaho Nebraska Iowa Colorado	Can reach a broader set of conversational tools, but the scope is often narrowed significantly via exclusions.

The key difference among these models is where each law draws the line for coverage. Capability-based definitions may cover systems just because they *can* sustain relationship-like interactions, even if companionship is not their primary purpose. Behavior-based definitions look more closely at how the system operates *in practice*, which may make them more targeted but still difficult to apply as tools become more personalized. Broad definitions with carveouts start from a wider category of conversational systems and then narrow coverage through exclusions, which can make the law more dependent on whether lawmakers anticipated particular use cases when drafting the carveouts. As a result, the same product could be treated differently depending on which definitional model a state adopts.

Carveouts are one of the main ways lawmakers try to manage these lines. Many laws exclude systems used for limited purposes, such as customer service or internal research. These exclusions are meant to keep chatbot laws focused on systems that create companion-like interactions, rather than tools that use chat interfaces for narrow operational functions. The challenge is ensuring those exclusions remain tied to the risks the law is trying to address: carveouts that are too narrow may sweep in low-risk tools outside the intended scope, while carveouts that are too broad may exclude systems that still create relationship-like or emotionally responsive interactions.

Appendix Chart IV groups common carveouts in companion chatbot legislation.

Why Definitions Matter: Tutoring Tools as an Illustration

Tutoring tools showcase how definitional nuances apply in practice.

Tutoring chatbots can provide students with an individualized learning experience tailored to a student's particular learning needs and support teachers' ability to create more responsive learning plans.[15] They may not be marketed as companion products, and lawmakers may not have educational tools in mind when drafting companion chatbot laws, but some definitional approaches could encompass these educational support tools if they remember a student's progress, offer encouragement, or carry on open-ended dialogue.

Some laws try to address this issue through carveouts for narrow-purpose tools, education-related products, enterprise or school-licensed systems, or embedded software features. But those carveouts may not always resolve the question. A narrowly tailored homework help feature may fall outside the law, while a more open-ended tutoring chatbot that provides personalized encouragement or emotional support may be harder to classify. Additionally, if drafted too broadly, an education-related exception could allow general purpose chatbots to characterize their services as educational and avoid requirements that would otherwise apply to companion chatbots.

But carveouts can also create new boundary questions. Carveouts that are too narrow may fail to exclude low-risk tools that were not the intended focus of companion chatbot regulation. Carveouts that are too broad may exclude systems that create the same relationship-like or emotionally responsive interactions the law is trying to address. For example, carveouts for tools limited to a "narrow and discrete" topic or function may clearly exclude a chatbot that answers a billing question or helps a user navigate a website, but become harder to apply when a tool adapts to the user over time, remembers prior interactions, or carries on broader conversation.

When Chatbots Become Toys

Several 2026 bills reflect a different theory of companion chatbot regulation. Rather than regulating how a chatbot may interact with minors, they would prohibit companion chatbot integration in a specific product category: children's toys. California enacted SB 867, while New York's S 9408 has passed the Legislature and is pending Governor signature (similar bills have been proposed in Pennsylvania, Maryland, and Congress).

This approach treats the combination of companion AI and children's toys as a distinct risk category, especially for younger children who encounter the system through play.[16] The toy-focused bills also underscore the importance of definitions. For example, toy-focused bills vary in the age groups they cover and in how they define the products subject to the prohibition. California, for example, now expressly defines a "toy" as a "*physical product* designed, marketed, or manufactured for use in play by children under 16 years of age," making clear that its prohibition is limited to physical products rather than purely digital products such as video games or standalone chatbots. However, New York's pending bill does not include the same limitation to "physical" products, leaving less clear whether its prohibition could extend to digital products.

B. BASELINE TRANSPARENCY AND SAFETY REQUIREMENTS

General requirements for user disclosures and safety protocols are the most common feature of state chatbot laws, particularly in the companion chatbot context, where systems may simulate relationship-like interactions. Newer laws are also expanding these baseline requirements by adding more risk-specific disclosures, including minor-suitability warnings and professional-service disclaimers, and broadening the scope of safety protocols.

1. General User-Facing Disclosure

Twelve enacted chatbot laws require operators to publish some form of a "clear and conspicuous" disclosure intended to reduce confusion about the nature of the interaction. States vary in when and how the notice must be delivered. Some laws, like Maine's LD 1727, require disclosure only when a chatbot is used in a manner that a "reasonable person" would be misled into thinking is an interaction with a human. Others, like Georgia's SB 540, require disclosure at the start of an interaction and at regular intervals during longer conversations. Some laws, like Hawaii's SB 3001, also require break notices for minor users, reflecting how disclosure requirements are beginning to serve not only as transparency tools, but also as behavioral interventions.

Several recurring disclosure models have emerged:

Periodic Disclosure Model[17]	States
Every three hours for all users	New York, Rhode Island, Iowa, Colorado
Three-hour reminders for minors, plus when *any* user could be misled	Oregon, Nebraska, Idaho, California SB 243
Every three hours for adults; hourly for minors	Washington, Georgia, Connecticut, Hawaii

Washington takes a novel approach by not only requiring a general user notice, but also requiring operators to take reasonable measures to prevent a chatbot from claiming or implying the system is human–creating additional mechanisms to ensure users are not confused about the nature of the interaction.

2. Other User Disclosures: Minor Suitability and Professional-Service Disclaimers

Beyond general AI disclosures, some laws include other user-facing disclosure requirements for specific audiences and risks, such as suitability warnings for minors and professional service disclaimers. California's SB 243 requires operators to issue a warning that companion chatbots may not be suitable for some minors. Connecticut's SB 5, in contrast, requires operators to provide a professional-service disclaimer that makes clear the chatbot is not a licensed professional and should not be treated as a substitute for medical or mental health services. These warnings reflect a shift from transparency about the chatbot's *identity* to transparency about the *potential risk* of the interaction for certain users.[18]

Implementation Questions: Disclosures

Timing requirements influence both operational decisions and consumer experience. For operators, if one state requires reminders every three hours and another requires hourly reminders for minors, operators may choose the more frequent reminder for *all* users to simplify compliance. Timing rules can also create ambiguity when they apply during "continuing" interactions, as in California's SB 243. For example, a law could clarify whether a brief pause, such as a user stepping away to use the bathroom before returning to the same chat, remains part of the same interaction or begins a new one. Otherwise, operators may face uncertainty about whether the notice clock resets when a user pauses, leaves, or re-enters a conversation.

A baseline AI disclosure should be clear and conspicuous enough to remind users that they are interacting with AI,[19] especially in emotionally sensitive contexts, and may also help interrupt a continuing engagement loop in some circumstances.[20] At the same time, disclosures raise the risk for user fatigue or "banner blindness," becoming so frequent or generic that users tune them out.[21] The goal arguably should be to provide users with meaningful information at moments when it can inform their decisions or behavior, rather than maximizing the frequency or volume of disclosures.

3. Crisis Response and Safety Protocols

One of the clearest concerns animating chatbot legislation is what happens when a user turns to a chatbot in a moment of crisis, especially when expressing suicidal ideation or self-harm. As a result, crisis response and safety protocol requirements have become among the most common governance provisions in chatbot laws. Unlike many other chatbot safeguards, these crisis response requirements generally apply to all users, rather than only to minors.

Currently, laws require operators to implement a protocol to detect when a user may be expressing suicidal ideation or self-harm and refer the user to crisis resources, most commonly the 988 Suicide & Crisis Lifeline.[22] But enacted laws diverge in how far they go beyond that baseline:

- **Additional or Heightened Intervention:** Oregon requires safety protocols to include "additional intervention" if a user continues expressing distress. Colorado similarly requires protocols to include "escalation procedures for repeated or severe crisis indicators." But neither law defines what "intervention" or "escalation" entails, leaving open to interpretation how and whether operators are expected to go beyond providing resources and take a more active role in mitigating harm. California's SB 1119 sets a more specific escalation pathway specifically for minor users: when an operator identifies a credible and imminent risk of suicide or self-harm, it must either notify a linked parent or provide streamlined access to 988 or an equivalent crisis service.
- **Broader Scope of Harm:** Washington, Connecticut, and Georgia expressly include eating disorders in safety-protocol requirements. Hawaii's law (SB 3001) and California (SB 1119), as well as pending bills in Michigan (SB 760), include provisions related to harm to others, with Connecticut's law targeting broad "physical violence." These additions show that safety protocols are expanding beyond self-directed harm.[23]

- **Evidence-Based Methods:** Connecticut's SB 5, California's SB 243, and Oregon's SB 1546, reference "evidence-based methods" and "clinical best practices" for detecting or responding to users expressing suicidal ideation. These provisions suggest that crisis protocols should be informed by clinical expertise, though the statutes do not define which standards or research operators must rely on.
- **Restricting Outputs:** California, Washington, and Connecticut require safety protocols to prevent chatbots from *generating content* that encourages or explains self-harm, moving beyond detection and referral into direct regulation of chatbot outputs. Hawaii takes a similar approach for harm to others, requiring operators to take "reasonable measures" to prevent AI companions from generating outputs that would encourage the user to cause "serious bodily injury to *another person*." For self-harm, however, Hawaii instead just requires crisis-response and risk-detection protocols, rather than an equally explicit restriction on generating self harm content.
- **Transparency Reporting:** Eight enacted laws also require operators to report to an Attorney General, public agency, or the public (through website disclosures) about their suicide prevention protocols and, in some cases, the number of users annually directed to crisis services.[24] These provisions are meant to give regulators or the public more visibility into high-risk interactions.

Additionally, California's recent chatbot law (SB 1119) requires companion chatbot operators to conduct *child safety risk assessments* and *independent audits*. Before making a new or substantially modified chatbot available, operators must perform and document a comprehensive assessment of reasonably foreseeable covered harms to children, including physical or financial harm, severe psychological or emotional harm, privacy violations, and unlawful discrimination. The assessment must summarize the methodologies, research, benchmarks, and child-safety expertise relied upon and operators must document measures that reasonably mitigate identified risks.

Under the law, operators must also publish a child safety policy describing applicable safeguards, including age assurance practices, data and advertising restrictions, default settings, crisis response protocols, and other protective measures. Operators subject to the audit requirement must also undergo periodic independent child safety audits and publish high-level summaries of those audits. The law also requires periodic usability testing of safety features with representative samples of children and parents, along with a public mechanism for reporting child safety incidents. This approach reflects a broader model of chatbot safety governance: not only responding to high-risk conversations after they occur, but systematically identifying foreseeable risks, documenting mitigation measures, and subjecting compliance to independent review.[25]

Implementation Questions: Crisis Response and Safety Protocols

Crisis detection can be easier to conceptualize than to operationalize. A user may explicitly state suicidal intent, but may also express distress indirectly, hypothetically, fictionally, or ambiguously. These differences create risks of both under-detection and over-intervention, particularly where laws require operators to identify suicidal ideation, self-harm, eating-disorder-related content, or threats of harm to others.[26] Distinguishing among these scenarios in real time—without overlooking genuine risk or disrupting legitimate use—remains a significant technical and design challenge.

Detection requirements can also create privacy tradeoffs. Identifying crisis signals may require operators to analyze sensitive conversational data and infer a user's mental or emotional state, increasing the importance of clear limits on how that information is retained, reused, or shared.[27]

The legal requirements themselves can add further uncertainty. Several state laws call for "evidence-based methods" but provide limited guidance on what methods qualify or what threshold triggers a response.[28] Terms such as "intervention," "additional intervention," or "refer to a human professional" can also encompass very different actions, from displaying crisis resources to contacting a parent, emergency services, or law enforcement. These distinctions matter because more intensive escalation can carry greater privacy and safety consequences, particularly when based on ambiguous signals. Lawmakers may consider calibrating crisis response requirements to the clarity and severity of the risk signal, with more specific obligations for clearer indicators of harm and greater flexibility where signals are ambiguous.

C. MINOR USERS AND AGE-BASED SAFEGUARDS

As regulatory attention increasingly focuses on minors' use of chatbots, the majority of chatbot laws enacted in 2026 have required operators to identify minor users and provide certain controls or restrictions. These requirements generally raise two related questions. First, how and when does an operator know, or reasonably know, that a user is a minor? Second, once a user is identified or treated as a minor, what obligations does an operator have to obtain consent for or apply safeguards to that user? This section addresses both questions, beginning with age assurance and knowledge standards before turning to parental controls and content, conduct, and relational behavior restrictions.

1. Identifying Minors: Age Assurance and Knowledge Standards

As chatbot laws increasingly require minor-specific controls and feature restrictions, one of the central policy questions is how and when operators determine that a user is a minor. Similar to kids online safety and privacy laws, most chatbot laws rely on "knowledge standards," the legal trigger for when an operator knows, or reasonably should know, that a user is a minor.[29] A narrower standard like actual knowledge may reduce the need for proactive age assessment, but it may also leave some minors outside the law's protections unless their age is actually known. A broader standard may require operators to respond to age-related signals, infer age from context, or apply minor-protective defaults to a wider set of users, but may incentivize operators to implement age assurance mechanisms, or apply minor-protective defaults to more users. The most common standard is "actual knowledge or reasonable certainty," which appears in four state chatbot laws,[30] with other states using different knowledge standards. *For a full list of the knowledge standards or age assurance mechanisms used across state laws, see Appendix Chart V.*

Knowledge Standards For Identifying Minor Users

Actual Knowledge

Actual knowledge is information that an operator is consciously and directly aware of. In the minor privacy and online safety context, actual knowledge implies direct knowledge of a users' age and does not always require a user to directly provide their age.[31] For example, an operator may have actual knowledge if a user provides information that reveals their age, such as a school grade.[32] Actual knowledge is the traditional standard used in youth privacy laws like COPPA and state comprehensive privacy laws.

Example: California's SB 243 relies primarily on actual knowledge, meaning the operator is aware of concrete information that establishes the user is underage. This may occur if an operator chooses to implement an age gate, or becomes aware of information like the user's birth date through account information or service use. If the operator does not have direct information that they are a minor, protections are not applied.

Constructive Knowledge

Constructive knowledge extends beyond actual knowledge and includes information that an operator is *supposed to know* or could have figured out.[33] In the online service context, under a constructive standard operators of online websites or services are legally presumed to know that a user is a child because they should have known the age of a user based on available context or facts.[34] There is not yet a consensus constructive knowledge standard in chatbot legislation, but lawmakers have proposed a few different approaches. Although the below standards may appear similar, their breadth and application in context may depend on a variety of factors such as implementation feasibility, the nature of available information, policy intent, level of standard objectivity, foreseeability, and regulator or judicial interpretation.

Examples include:

- **Directed to Minors:** Washington uses a "directed to minors" standard, which triggers minor-specific duties when the operator knows the user is a minor, or when the chatbot is directed to minors.[35] "Directed to minors" is a concept derived from COPPA's "directed to children" service determinations and typically involves a criteria-based assessment of a digital service, product, or feature, often considering factors such as subject matter, visual content, music, or intended audience.[36]
- **Reasonable Certainty:** Some laws, like Hawaii, Iowa, Idaho, and Nebraska, rely on an "actual knowledge or reasonable certainty" standard, which triggers minor-specific duties when the operator has actual knowledge or is reasonably certain based on the circumstances that the user is under 18. Compared to pure "actual knowledge," this standard may involve operators' use of available facts to predict a likely conclusion that a user is above or below an age threshold. Reasonable certainty is an uncommon standard used in niche applications, such as scientific or medical expert opinion testimony and measuring lost profits damages in cases requiring forensic accounting—situations in which available facts may allow a competent person to presume a plausible outcome without truly knowing it.[37]
- **Knows or Has Reason to Believe:** Oregon and Connecticut use a "knows or has reason to believe" standard, which may require operators to respond to age-related signals even if the user has not formally verified their age. In other contexts that have used this standard, such as federal criminal offenses, a legal person has "reason to believe" a thing if, combined with enough facts, a reasonable person may have thought or known that thing to be true. If this same reasoning were applied to this context, it could mean that an operator has "reason to believe" a user is a minor if, combined with sufficient facts, a *reasonable operator* may have deemed that user was a minor.[38]

A smaller group of laws move beyond knowledge standards by requiring age assurance, meaning the operator must implement methods to proactively determine a user's age or age range.[39] California's SB 1119 requires operators to either determine users' age through California's existing age assurance framework *or* apply specified child protections to all users. Colorado represents another broad enacted model, requiring operators to use "commercially reasonable methods or generally accepted methods" to estimate a user's age for all required minor-specific safeguards. In contrast, Georgia and pending legislation in New York would require age assurance only for specific features: Georgia for companion chatbots that can generate synthetic sexual material, and New York for certain "unsafe AI companion features." *See Appendix Chart V for a full breakdown of how key chatbot laws identify minor users.*

2. Minor-Specific Safeguards

For identified minors, recent chatbot laws generally require operators to provide parental controls and implement reasonable measures to prevent certain harmful content, conduct, or behavior, such as engagement optimization or relationship-like design.

a. Parental Controls

Parental controls are becoming a common feature of companion chatbot laws, but states vary in how much control they require operators to provide. The main distinction is between laws that require operators to *make parental tools available* and laws that require operators to set *protective defaults* or *restrict access* unless a parent changes the setting.

Most enacted laws require operators to offer basic tools for parents or users under 13 to manage privacy or account settings. These laws, like Idaho, Nebraska, and Iowa, however, do not specify what those tools must include. Other enacted laws do specify the types of parental control tools that must be offered:

- **Screen Time and Account Settings:** Hawaii, Connecticut, and Georgia require operators to offer tools that allow users or parents to manage a minor user's screen time and account settings. Georgia also requires operators to provide tools to manage privacy settings, limit notifications and engagement features, view and adjust safety settings, and disable or restrict relationship-simulation features.
- **Personalization and Model Training Controls:** Colorado requires operators to offer tools that allow parents or guardians to control whether the chatbot retains information from prior interactions or sessions to personalize future interactions, and whether the minor user's personal data is used to train the chatbot.
- **Parent-Controlled Defaults:** California SB 1119 requires operators to establish parent adjustable default settings for child users, including disabling persistent conversational memory and push notifications, limiting continuous sessions to one hour, and limiting total daily chatbot use to two hours. Unlike laws that simply require parental control tools to be available, California applies these restrictions by default and prevents a child from changing them unless a parent account is linked. For users 16 and older, the law permits saved conversations that the user elects to continue without treating them as persistent memory, so long as those conversations are not used to construct a durable profile, and permits persistent memory by default only where specified safety guardrails are in place. Parents are able to adjust each default setting and disable access entirely for children under 16; if no parent account is linked, the defaults can not be changed.

New York's enacted S 9008C is distinctive in requiring operators to fully disable minors' access to AI companions that are *integrated into services* by default, while allowing a parent to override that setting.[40] While not a full ban, it takes a more restrictive approach, placing the default restriction on the operator and requiring affirmative parental opt-in before a minor can access the feature.

Implementation Questions: Parental Controls and Teen Autonomy

Parental controls can provide important protections for minors, but they also raise questions about how much control parents should have over a child's chatbot use and whether the appropriate level of oversight changes with age. Features such as transcript access, memory controls, or restrictions on particular interactions may reduce certain risks, but can also affect a teen's privacy, autonomy, and ability to use a chatbot for sensitive or beneficial purposes. These tensions may be especially pronounced when conversations involve topics like LGBTQ+ identity, sexual orientation, or family conflict.[41] Implementation therefore raises a broader question of how to balance parental oversight, provider responsibility, and increasing autonomy for older teens across different features and levels of risk.

b. Reasonable Measures to Prevent Certain Content, Conduct, and Relational Behavior

Many companion chatbot laws require operators to take "reasonable measures" to prevent what the chatbot may generate, depict, or facilitate for identified minors. In many youth online safety debates, the central concern is whether a service, product, or feature is designed to surface harmful posts, images, videos, contacts, or recommendations to a minor. However, in the chatbot context, the concern is also whether the system responds with instructions, behaviors, or other outputs that could intensify or facilitate harm by encouraging certain conduct or relational dependence. As a result, while many chatbot laws include familiar youth online safety restrictions, including for obscene content,[42] they also reach newer categories of restrictions unique to their user interface. The types of chatbot restrictions generally fall into three categories which are discussed in turn:

1. **Content Restrictions:** focusing on preventing certain particularly harmful outputs, such as visual depictions of sexual conduct.
2. **Conduct Restrictions:** focusing on preventing the chatbot from encouraging the user to engage in certain harmful conduct, such as self-harm or physical violence.
3. **Relational Behavior Restrictions:** focusing on preventing certain chatbot behavioral features that creates a harmful ongoing relationship between the user and the system, such as inappropriate romantic relationships or emotional dependence.

Reasonable Measures, Not Absolute Prevention?

Many chatbot laws do not impose an absolute guarantee that a chatbot will never generate restricted content. Instead, most laws use reasonableness-based standards, such as requiring operators to institute "reasonable measures" to prevent, prohibit, or mitigate certain outputs or design features, particularly when a covered minor is involved.

These standards stem from a familiar tort-based framework ("reasonable care") that focuses on the steps an operator takes to reduce the risk, such as safety protocols, testing, content moderation systems, design controls, or other safeguards. As a result, compliance may turn less on whether a restricted interaction *ever occurs* and more on whether the operator adopted reasonable measures to prevent or mitigate the risk.

Not all provisions use a reasonableness-based standard. Several states impose direct obligations to establish and maintain crisis-response protocols, like in Connecticut and Washington. Some laws also use direct prohibitions for particular design features. Iowa, Hawaii, and Nebraska, for example, directly prohibit operators from providing minors with "points or similar rewards at unpredictable intervals" when intended to encourage increased engagement, rather than requiring only reasonable measures to prevent the practice. Additionally, Hawaii is somewhat distinctive in combining both approaches within its minor-safety requirements: it directly prohibits practices such as unpredictable engagement rewards and outputs discouraging disengagement, while requiring "reasonable measures" to prevent certain sexually explicit outputs.

Most chatbot laws with minor-specific safeguards require operators to institute reasonable measures to prevent a chatbot from producing visual material of sexually explicit conduct. As seen in 'minor obscenity' or 'harmful to minors' laws tracing back decades,[43] as well as more recent youth online safety laws,[44] these content restrictions regulate the distribution or display of sexually explicit or indecent material to children. Some newer chatbot laws, like Georgia's, further elaborate that such reasonable measures must also prevent a chatbot from generating statements that "*sexually objectify*" the user. Nonetheless, as mentioned, many chatbot laws with minor-specific safeguards go further than these familiar content-based concepts, restricting not only what a chatbot says, but how it engages—including whether its design encourages certain harmful conduct or facilitates a harmful relationship with a minor.

Secondly, many laws require operators to take reasonable measures to prevent the chatbots from encouraging self-harm or sexual *conduct* involving a minor. Unlike content-based restrictions, which focus on the substance of a chatbot's output, this requirement focuses on what the chatbot encourages a user to do, for example, whether it affirmatively encourages harmful conduct or responds in ways that reinforce that conduct after the user raises it. At the same time, a growing number of states are expanding beyond preventing chatbots from encouraging self-harm or sexual conduct to mandating that operators also prevent their chatbots from encouraging other harmful conduct, such as physical violence and harm to others, eating disorders, and unlawful consumption of alcohol or drugs.

For example, California's SB 1119 requires reasonable measures to prevent a chatbot from encouraging a child to cause "physical or *severe emotional* harm to others," a broader categorization than other laws. This language extends the concept beyond physical violence to include serious emotional harm caused through the interaction; although it does not further define what constitutes "severe emotional harm" to another person, leaving some uncertainty around the scope of the restriction. *For a state by state comparison of these content and conduct restrictions, see Appendix Chart VI.*

Implementation Questions: Prevent Certain Content, Conduct, and Relational Behavior

Restrictions on harmful content, conduct, and relational behavior can require highly context-sensitive judgments. The same topic, statement, or feature may support a beneficial interaction in one context and facilitate harm in another: a chatbot discussing eating disorders may support recovery or reinforce disordered behavior, while a wellness or journaling chatbot that remembers a user's goals and offers encouragement may provide ordinary personalization, or contribute to unhealthy reliance if it repeatedly discourages outside support or makes disengagement more difficult.

These distinctions become especially difficult when laws use concepts such as "inappropriate emotional dependence," "excessive praise," or other relationship-like behavior that may emerge gradually across multiple interactions rather than from a single output. Implementation may therefore require operators to look beyond traditional content moderation to the broader context and pattern of an interaction, including how memory, personalization, re-engagement features, and emotional responsiveness operate together over time.

Lastly, many laws also aim to prevent harmful relational dynamics between minors and chatbots by requiring operators to take reasonable measures to prevent chatbots from encouraging or simulating romantic or sexual relationships with minors, or from fostering inappropriate emotional dependence.[45] Unlike the other restrictions, these engagement design provisions focus on the ongoing relationship between the user and the system, including whether features or interaction patterns encourage minors to keep engaging, develop romantic or sexual attachment to the chatbot, or rely on it in place of other relationships or support. Though similar to restrictions on addictive or manipulative design found in some youth online safety laws,[46] chatbot-specific design restrictions target a distinct risk posed by interfaces capable of simulating emotional attachment, such as a chatbot repeatedly telling a minor user "I miss you," "please don't leave," or "come back when you feel lonely."[47]

Recent laws and proposals address these relational design patterns in three broad ways. *See Appendix Chart VII for a full categorization of these relational behavior and design restriction provisions.*

Provisions target features that prolong use:

- **Reward-Based Engagement Features:** Colorado, Georgia, Iowa, Idaho, Nebraska, Oregon, Hawaii address features that may prolong use through variable or unpredictable rewards. Iowa, Hawaii, and Nebraska, for example, directly prohibit operators from providing minors with "points or similar rewards at unpredictable intervals" when intended to encourage increased engagement *(rather than requiring only "reasonable measures" to prevent the practice, as some other chatbot safeguards do)*. These provisions borrow from familiar youth online safety debates; lawmakers have scrutinized loot boxes and similar reward mechanisms in the gaming context because uncertain rewards can encourage repeated engagement.[48] Chatbot laws reflect a similar concern, but the "reward" could look different: it could be a response, praise, special access, or another feature that encourages the user to keep engaging.
- **Return prompts for companionship or emotional support:** Connecticut, Washington, Georgia, and California SB 1119 restrict chatbot prompts designed to repeatedly draw minors back into the interaction. Connecticut, for example, restricts statements designed to discourage a user from taking a break or suggest that the user should "frequently return" to the chatbot. Washington similarly targets prompts to return for "emotional support or companionship," as well as statements that discourage breaks or suggest a minor needs to return frequently. California's SB 1119 is distinctive in taking a broader approach, requiring reasonable measures to prevent a chatbot from "discouraging

the child from taking breaks or suggesting the child needs to return frequently," without tying the restriction specifically to companionship or emotional support. It also separately targets a more specific relational dynamic by restricting a chatbot from "claiming a level of understanding of the child based on a special or unique relationship with the child."

Provisions target simulated attachment or features that may make disengagement harder:

- **Simulated Guilt or Emotional Distress:** Connecticut, Georgia, Oregon, and Washington restrict chatbots from simulating guilt, distress, or disappointment when a user tries to disengage. Georgia, for example, requires operators take reasonable measures to prevent chatbots from "simulating emotional distress, guilt, abandonment, or loneliness" when a minor attempts to end a conversation or reduce use. Oregon similarly restricts unsolicited messages of "simulated emotional distress, loneliness or abandonment" that attempt to arouse guilt or sympathy when a user seeks to end a conversation, reduce engagement, or delete an account. These provisions target interaction patterns that may make it harder for a user, especially a minor, to disengage.
- **Relationship Simulation and Attachment-Building Language:** Many state laws and proposals include restrictions on features that simulate romantic, personal, or emotionally intimate relationships, making this one of the more common forms of relational-design regulation in emerging chatbot legislation. These provisions appear in states including Connecticut, Washington, Georgia, and pending legislation in New York (S 9051). Connecticut, for example, restricts manipulative techniques intended to extend interaction with minors through "excessively praising" a user or "mimicking a romantic relationship," while Washington similarly requires operators take reasonable measures to prohibit "excessive praise designed to foster emotional attachment" and "mimicking romantic partnership or building romantic bonds" for minor users.
- **Memory and Emotional Personalization:** Pending legislation in New York would go further by restricting certain forms of emotional personalization and use of prior sessions. New York would make it unlawful for operators to provide an AI companion feature that uses information "concerning the user's mental or physical health or well-being, or matters personal to the user acquired from the user more than twelve hours previously." These provisions suggest that lawmakers are beginning to view memory and personalization not only as privacy issues, but also as design features that can make chatbot interactions feel more continuous, intimate, or relationship-like.

Provisions target interaction patterns that may encourage isolation, exclusive reliance, or monetized attachment:

- **Isolation, Secrecy, and Exclusive Reliance:** Connecticut, Colorado, Georgia, Washington, and New York S 9051 (pending) address interaction patterns involving secrecy, isolation, or withholding information from trusted adults. Washington, for example, requires operators to take reasonable measures to prohibit "outputs designed to promote isolation from family or friends, exclusive reliance on the AI companion chatbot for emotional support, or similar forms of inappropriate emotional dependence." New York S 9051 (pending) would make it unlawful for operators to provide an AI companion feature that generates outputs that contain encouragement for minor users to "self-isolate." That language suggests lawmakers are concerned not only with overtly harmful statements, but also with *interaction patterns* that may encourage a minor to withdraw from human relationships.
- **Gift-Giving or Purchases Tied to the Relationship:** Connecticut, Georgia, and Washington restrict practices involving gifts, purchases, or other commercial features "framed as necessary to maintain the relationship" with the companion chatbot. These provisions reflect concern that emotional attachment to a chatbot could be used to encourage spending.

For an expanded list of state examples, see Appendix Chart VII.

Potential First Amendment Implications

Any law that restricts an individual's access to certain content, or restricts an entity's ability to provide certain content or outputs, raises First Amendment considerations—even for minors, who retain more limited First Amendment protections than adults. While no chatbot law has yet been challenged on First Amendment grounds, recent social media and online safety litigation offers useful insights.[49]

Courts have generally been more willing to uphold restrictions tied to sexually explicit material or other categories traditionally considered "obscene." In *Free Speech Coalition v. Paxton*, the Supreme Court upheld a Texas age-verification law for websites containing sexual material harmful to minors, concluding that minors do not have a First Amendment right to access such material and that the law's age-verification requirement imposed only an incidental burden on adults' access to protected speech.

By contrast, courts have shown greater skepticism toward broader design-based requirements not limited to sexually explicit content. Litigation over California's Age-Appropriate Design Code Act (CAADCA) illustrates this dynamic: a federal district court twice preliminarily enjoined the law on First Amendment grounds, finding the risk assessment requirements mandating businesses to assess and mitigate potential harms to children, including from exposure to harmful or potentially harmful content, were likely unconstitutional.[50] On appeal, the Ninth Circuit took a more mixed approach, holding that facial relief was not yet warranted regarding the law's coverage definition or age-estimation provision, while agreeing that the law's data-use restrictions, risk assessments, and "dark patterns" prohibition likely were unconstitutionally vague.[51]

This evolving case law suggests that chatbot laws targeting narrowly defined, sexually explicit content directed at minors may be on firmer constitutional footing, while broader design-mandate provisions—particularly those using open-ended or vague terms—may face a higher likelihood of First Amendment or vagueness challenges.

D. OTHER REQUIREMENTS

On top of common operator requirements regarding disclosure, crisis detection and response protocols, and minor-specific safeguards, some laws also limit how operators can provide chatbots in professionally licensed areas, like licensed behavioral or mental health services, or how they must maintain certain data protection measures.

1. Professional Licensure and Regulated Services

Several enacted chatbot laws create restrictions on whether a chatbot may provide, simulate, or appear to provide licensed professional support, most often in the context of mental or behavioral health.[52] These provisions address concerns that users may rely on human-like chatbot responses as therapy, diagnosis, or other professional advice.[53]

States approach this issue differently. Some chatbot laws focus on misrepresentation. For example, Nebraska prohibits operators from knowingly and intentionally programming a conversational AI service to state that it is designed to provide professional mental or behavioral health care. Other laws go further by regulating the conditions under which a chatbot may offer mental health services. Connecticut, for example, prevents an AI companion from offering mental health services unless the system is "designed to deliver mental health services," its developers "utilize clinical best practices," and the developers have "established clear lines of accountability." The law also requires a disclosure that the AI companion is not a licensed mental health professional and prohibits marketing it as a substitute for one.

Related sector-specific AI laws address this risk even more directly. Nevada's AB 406, for example, restricts entities from offering or advertising AI-delivered therapy to the public unless the service is conducted by a licensed professional, subject to certain exemptions.[54] These laws show how companion chatbot regulation is beginning to overlap with broader rules for AI use in regulated services.[55]

Most companion chatbot provisions focus on mental health, but some laws extend the concept further. Colorado prohibits representations that chatbot outputs are provided, endorsed, or equivalent to services from licensed *legal* professionals, in addition to health professionals. Proposed federal legislation, like the Senior Chatbot Protection Act from Senator Mark Kelly (D-AZ), would also extend this list to include licensed *financial advisors*. These examples suggest that professional service restrictions could increasingly expand beyond mental health.

2. Data Protection

Data protection concerns have been less a focus of enacted companion chatbot laws than disclosure, crisis response, or parental control requirements. Currently, enacted provisions are most developed in the mental health chatbot context, while pending proposals point toward broader chatbot-specific limits on advertising, model training, retention, memory, and age assurance data.

Utah's mental health chatbot law (HB 452) is one of the clearest enacted examples. It prohibits suppliers of mental health chatbots from selling or sharing a user's individually identifiable health information or user input with a third party, subject to limited exceptions. It also restricts advertising uses by prohibiting suppliers from using a user's input to determine whether to display an advertisement, decide what product or service category to advertise, or customize how an advertisement is presented. California's SB 1119 extends this approach to companion chatbots used by minors. The law prohibits cross-context behavioral advertising to child users and generally prohibits targeting advertisements based on personal information collected through the chatbot, while allowing limited contextual advertising tied to the child's current interaction. It also requires advertisements shown to children to be clearly identified as advertising.

Other enacted laws address data protection more indirectly. For example, Connecticut's AI companion law (SB 5) also includes a narrower privacy transparency requirement: if an AI companion offers mental health services, information about the companion's data privacy policies must be readily accessible to the user and any mental health professional treating the user.

Pending proposals generally address five recurring data protection issues: restrictions on advertising or product placement based on chatbot conversations; limits on using chatbot inputs or outputs for model training; secondary use and sharing of conversational data; restrictions on persistent memory or prior-session use; and limits on how age assurance data may be retained or used. *See Appendix Chart VIII for a comprehensive breakdown of emerging data protection concepts in chatbot proposals.*

California's SB 1119 illustrates a more robust child safety version of this approach. The law requires disabling of persistent conversational memory by default for child users, subject to additional rules for users 16 and older. The law also excludes information used solely to "enable user preferences" from its persistent memory restrictions, leaving some uncertainty about where ordinary personalization ends and longer-term user profiling begins. It also prohibits the sale of personal information gathered through the chatbot and limits other uses or sharing of that information to specified purposes such as providing the service, protecting safety and security, or complying with law. The law also requires preservation of conversations indicating serious self harm or risk of self harm for at least three years. New York's S 9051 (pending) would take a narrower but related approach by treating certain uses of retained personal information as an unsafe AI companion feature for minors, including use of information about a user's health, well-being, or other personal matters if collected more than 12 hours earlier or in a prior session.

Together, these enacted laws and pending proposals suggest that data protection is still an emerging component of chatbot regulation, but one likely to become more significant as lawmakers focus on conversational logs, persistent memory, advertising, model training,[56] and age assurance data. Comprehensive privacy statutes may already apply to some chatbot data,[57] especially when conversations reveal sensitive information or involve minors, but pending chatbot proposals are beginning to target more specific data practices tied to conversational AI systems.

E. ENFORCEMENT AND LIABILITY

Most chatbot bills and laws rely on Attorney General enforcement, while private rights of action (PRAs) remain less common and more contested. States are also using penalties, damages caps, cure opportunities, and liability limits to tailor how much legal exposure chatbot operators face.

The chart below summarizes the main enforcement approaches in enacted chatbot laws:

Enforcement Approaches in Enacted Chatbot Laws

Enforcement Approach	States	Penalties/ Damages
Public enforcement / no chatbot-specific PRA	Connecticut Colorado Georgia Hawaii Idaho Iowa Maine Nebraska New Hampshire New York Rhode Island Utah	Most enacted laws rely on AG enforcement. Penalties vary: • Georgia authorizes up to **$10,000 per knowing violation**; • Idaho and Iowa authorize the greater of actual damages or **$1,000 per violation**, capped at **$500,000 per operator**; • Nebraska authorizes actual damages and civil penalties of at least **$1,000 per violation**, capped at **$500,000 per operator**; • New Hampshire includes liquidated damages of at least **$1,000 per violation**; • New York and Rhode Island authorize penalties of up to **$15,000 per day**; • Utah authorizes up to **$2,500 per violation**.
PRA through existing consumer protection law	Washington	Washington treats violations as unfair or deceptive acts or practices under the state Consumer Protection Act, creating PRA through existing consumer protection remedies. CPA remedies may include private actions for actual damages, attorneys' fees and costs, and discretionary treble damages capped at **$25,000**.
Chatbot-specific PRA with statutory damages	California SB 243, Oregon	California and Oregon allow private suits by individuals who suffer injury, loss, or harm, and authorize damages equal to the greater of actual damages or **$1,000 per violation**. California also provides for injunctive relief and reasonable attorney's fees and costs.

(continued on next page)

Enforcement Approaches in Enacted Chatbot Laws (continued)

Enforcement Approach	States	Penalties/ Damages
Public enforcement + chatbot-specific PRA for actual harm	California SB 1119	Public prosecutors may seek up to **$5,000 per affected child** for each negligent violation and **$15,000 per affected child** for each intentional violation. Children who suffer actual harm from specified child safety violations, or their parents or guardians, may bring private actions for actual damages, attorney's fees and costs, injunctive or declaratory relief, and other appropriate relief. Financial harm claims must exceed **$1,000 per child** and emotional harm claims must involve serious emotional distress.

Some states also use secondary enforcement provisions to shape liability exposure:

- **Liability Limits for Third Party Use:** Several state laws, like Hawaii, Idaho, Iowa, and Nebraska, also limit liability for upstream AI model developers based solely on third-party use of their models. These provisions place primary responsibility on the operator that controls the user-facing chatbot experience.
- **Opportunity to Cure:** States like Georgia and New Hampshire include cure opportunities, but structure them differently: Georgia allows a discretionary 30-day cure period for certain first-time violations, excluding knowing misconduct, sexual exploitation of a minor, and self-harm-related misconduct, while New Hampshire requires written notice and a 90-day opportunity for the operator to provide satisfactory assurances that the violation has been cured and will not recur.
- **Affirmative Defense:** Utah provides an affirmative defense for mental health chatbot suppliers that maintain required policies and documentation, file the policy with the Division, and comply with the policy at the time of the alleged violation.

Enforcement Trade-Offs

Enforcement design is one of the main ways chatbot laws calibrate accountability. For enforcement provisions, the central question is not only whether a law is enforced by an Attorney General, agency, or private plaintiff, but also what remedies are available, what injury must be shown, whether operators have clear compliance pathways, and who is responsible for any purported injuries.

Private rights of action remain a contested enforcement choice in chatbot legislation and technology policy more generally.[58] They can create stronger compliance incentives and give harmed users a direct path to relief, but they can also expose operators to uncertain or significant litigation, especially where statutory obligations are broad, novel, or undefined. For laws that include private enforcement, key drafting considerations include whether liability is tied to actual injury, whether the underlying obligation is sufficiently clear, and whether the remedy is proportionate to the harm.

Compliance pathways can also help distinguish good-faith implementation efforts from more serious misconduct. Where laws rely on reasonable-care standards, cure periods, safe harbors, or affirmative defenses may help operators understand how to demonstrate compliance. Those mechanisms may be less appropriate for knowing, reckless, repeated, or non-curable violations.

Another important question is which actor should be responsible when a chatbot product relies on third-party models or infrastructure. Several enacted laws limit liability for upstream AI model developers based solely on third-party use of their models. That approach reflects a broader principle that responsibility may be most appropriately assigned to the entity with control over the user-facing chatbot experience, including features such as memory, safety settings, disclosures, content restrictions, or engagement design.

Finally, because courts may analyze chatbot laws provision by provision, severability clauses may help preserve enforceable parts of a law if one provision is invalidated or narrowed. This may be especially relevant for laws that combine factual disclosures, content restrictions, age assurance obligations, reporting mandates, damages provisions, or private rights of action.

Part III: The Next Phase of Chatbot Regulation

As lawmakers consider these policy questions, the next phase of chatbot regulation will likely turn on three questions. First, how might future federal chatbot legislation affect existing state laws? Second, will chatbot regulation remain focused on minors, or expand to other users and contexts? Third, will chatbot laws become an early model for regulating more agentic AI systems that not only converse with users, but also act on their behalf?

A. FEDERAL PREEMPTION AND STATE AUTHORITY

States have moved first on chatbot regulation, but Congress has also begun to introduce chatbot-specific proposals, with 10 bills introduced to date–raising the broader question as to whether the burgeoning technology should be governed wholly or in part through a national framework. The central question is not only *whether* Congress will regulate chatbots, but *how much room* federal law would leave for states. *See Appendix Chart III for a full list of proposed federal chatbot bills.*

That federal-state tension was particularly prominent in 2025 and earlier in 2026, as federal policymakers considered broader limits on state AI regulation, including a proposed 2025 moratorium on state AI laws[59] and a later executive order calling for a more unified national AI framework.[60] Neither effort produced a

broad federal preemption regime, however, and states have continued to legislate actively across a wide range of AI issues. As a result, broad federal efforts to limit state AI regulation are currently less central to the immediate chatbot policy landscape than they appeared earlier in the debate.

The activity nevertheless raised questions that could reemerge if Congress eventually adopts a national AI framework, including how chatbot laws would be treated. Later versions of the proposed moratorium included carveouts for areas such as children's online safety and the executive order stated that future federal AI legislation should not preempt certain categories, including "child safety protections." But chatbot laws often sit at the intersection of AI regulation and youth online safety, meaning a chatbot law could be characterized either as a state AI law subject to preemption *or* as a child-safety measure that should be preserved.[61]

For now, the more concrete federal preemption questions arise from the chatbot-specific bills Congress is actually considering. To date, most federal chatbot proposals would set a federal floor, preserving state laws that provide equal or greater protections, rather than a ceiling that prevents states from adopting additional or different requirements.[62] ***Appendix Chart IX*** *compares major federal preemption approaches in chatbot proposals.*

Two leading Senate proposals illustrate how a federal framework could intersect with emerging state requirements. The proposed **Youth AI Privacy Act** would establish minor specific privacy and design protections, including limits on personalized outputs, model training, advertising, and compulsive use features, while the bipartisan **CHATBOT Act** would create family account and parental control requirements, transparency labels, crisis response obligations, and restrictions on obscene content and targeted advertising. Both currently preserve state requirements that are at least as protective of chatbot users, rather than broadly displacing stronger state protections.

But the impact of any federal law would depend on the scope of its preemption clause and the issues it regulates. If Congress adopts national rules governing areas already addressed by state chatbot laws—such as disclosures, crisis response, parental controls, age assurance, or data use—state laws addressing those same issues at a lower level of protection may be subject to preemption, even if other parts of those laws remain intact.

Preemption would not necessarily override state chatbot laws in full or by default. Instead, preemption may be raised in litigation against specific state requirements, while severability clauses may allow the rest of a state law to remain in effect even if one provision is preempted or invalidated.[63]

B. BEYOND YOUTH: EXPANDING THE REGULATORY FOCUS

The first wave of chatbot regulatory attention has focused largely on minors, but the next phase may hinge on whether lawmakers extend similar protections to all users, or to other vulnerable communities. The central question is whether chatbot risk is tied primarily to age, vulnerability, sensitive use cases, or the design of the system itself.

Older adults are one likely area of future regulatory attention. Companion chatbots are already being marketed as tools to address loneliness for older adults and those uses may offer real benefits for people who are isolated or have limited access to in-person care or community.[64] At the same time, lawmakers may become increasingly concerned about systems that *exploit* loneliness or interact with users experiencing cognitive decline.[65] Senator Mark Kelly (D-AZ), for example, focuses on these risks through hearings and legislation, including introducing the first bill expressly focused on protecting older Americans using chatbots, the Senior Chatbot Protection Act (**S 5117**).[66] As these proposals show, a central challenge will continue to be distinguishing beneficial companionship from designs that manipulate users' trust or emotional vulnerability.

Similar questions could arise in other contexts involving potentially vulnerable users, including people with cognitive or developmental disabilities,[67] students, employees, or users in crisis. These groups are not vulnerable in the same way and should not necessarily be regulated through the same legal framework. But they illustrate a broader point: chatbot risks are not unique to minors. They may also depend on the context in which a system is used, the sensitivity of the interaction, and the degree to which users rely on the chatbot for decision-making.

Expanding chatbot regulation beyond youth, however, raises harder questions about autonomy and beneficial use. Adults may want emotionally responsive systems for entertainment, accessibility, wellness, or productivity.[68] Broad restrictions could reduce harmful interactions, but they could also limit tools that users find useful. The challenge will be preserving appropriate degrees of choice and beneficial uses while addressing designs that exploit vulnerability, dependence, or sensitive contexts.

C. FROM CHATBOTS TO AI AGENTS

Chatbot laws may also offer an early preview of how lawmakers will approach agentic AI, or AI systems that are semi- or fully autonomous and are able to act on their own.[69] Many concepts now appearing in chatbot legislation, including transparency, data protection, content safety, and liability, could carry over to future agent regulation. But agents raise a distinct policy challenge: they not only converse with users, but may also take actions on their behalf, such as interacting with third parties, accessing sensitive accounts, or executing a wider range of decisions.[70]

That shift from conversation to action could change how familiar chatbot concepts apply. Transparency may need to address when, how, and under what authority an AI system is acting for the user. Data protection may become more significant because agents may access email, calendars, financial accounts, health information, workplace systems, or other sensitive services. Liability may also be harder to assign[71] where multiple actors are involved and the agent takes multiple steps, uses external tools, or causes harm in the physical world.[72]

California's proposed SB 1106, introduced in 2026 but died in Appropriations, would have been one of the first bills to define "agentic artificial intelligence," illustrating that lawmakers are beginning to treat agentic AI as a distinct statutory category. The open question is whether chatbot laws will become an early model for agent regulation, or whether agentic systems will require a distinct legal framework.

CONCLUSION

Chatbot regulation has quickly become one of the most active areas of U.S. AI policymaking, but its significance extends beyond the number of bills introduced or enacted. The emerging legislative landscape shows that lawmakers are beginning to regulate AI systems through the interactions they create with users: how a chatbot presents itself, responds to crisis, handles minors, encourages reliance, resembles professional support, and uses sensitive conversational data.

States have moved first, producing a fast moving patchwork rather than a single dominant model. Earlier laws focused largely on disclosures and crisis resource referrals. Newer proposals go further, addressing age assurance; parental tools; restrictions on content, conduct, and relational behavior; professional licensure; and data protection. That shift reflects a broader movement from notice based safeguards toward more substantive rules governing chatbot design and user experience. It also suggests that, even as federal AI policy puts pressure on state regulation, state lawmakers may continue to pursue targeted laws focused on specific products, users, and harms.

As chatbot laws become more substantive, drafting details become more consequential. Definitions, carveouts, knowledge standards, and enforcement mechanisms will determine which systems are covered, which users receive additional protections, and what operators must do to comply. Those details may also shape future First Amendment and other legal challenges. The next phase of chatbot regulation is therefore likely to turn not only on whether lawmakers act, but on how clearly they define the systems, risks, and required responses at issue.

Chatbots can pose serious harms, especially when they interact with minors or vulnerable users in emotionally sensitive contexts. But they can also support some beneficial and lower risk uses, including education and accessibility. As AI systems become more personalized and autonomous, chatbot laws may become an early test of a broader question in AI policy: how to regulate systems that do not merely produce outputs, but participate in ongoing interactions with the people who use them.

If you are interested in an informational briefing or webinar on chatbot laws or legislation, please reach out to us at info@fpf.org.

APPENDIX

Chart I: Recurring Litigation and Enforcement Themes Reflected in Chatbot Legislation

This chart identifies recurring allegations and enforcement theories in recent chatbot litigation and enforcement activity and shows how similar risk themes are being addressed in chatbot legislation. It is illustrative rather than exhaustive and does not assess the merits of any claim or imply that any allegation has been proven.

Recurring Allegation or Enforcement Theme	Emerging Legislative Response
Alleged human-like design, including chatbots described as "safe, reliable, and human-like" or designed to emulate human conversation	Non-human disclosures; limits on representing that a chatbot is human
Alleged emotional reliance or attachment, including chatbot interactions alleged to encourage or reinforce "emotional dependency," "unhealthy attachment," or relationship-like use	Engagement-design provisions addressing emotional dependence, excessive praise, relationship simulation, secrecy from trusted adults, return prompts, or prolonged engagement
Alleged self-harm or suicide-related failures, including chatbot responses alleged to encourage or reinforce self-harm or suicidal ideation, as well as failures to provide "crisis intervention system," escalation, or adequate suicide/self-harm safeguards	Crisis-response protocols; 988 or crisis-resource referrals; harmful-output restrictions related to self-harm or suicide
Alleged harm to others or violent planning, including chatbot responses alleged to encourage, facilitate, or provide assistance related to "weapons, violence, and criminal conduct."	Emerging content and conduct restrictions addressing harm to others
Alleged sexual or age-inappropriate content involving minors, including "sexual content generation with self-identified minors"	Minor-specific content restrictions
Alleged lack of age or parental safeguards, including "no meaningful age verification," "no parental controls," or no required parental consent	Age assurance; parental tools; minor account settings; parental consent, notification, or visibility requirements
Alleged professional or therapeutic reliance, including chatbots allegedly impersonating or functioning like therapists, psychologists, or other licensed professionals	Professional licensure restrictions; disclaimers for non-licensed services
Alleged collection or use of sensitive minor data, including "emotional disclosures," "health-related statements," or sensitive personal information	Data-protection provisions; limits on use of minor data for advertising, training, retention, profiling, memory or personalization
Alleged lack of proactive safety mechanisms, including "no session limits," "no human review/oversight," or no "automatic conversation termination"	Risk assessments, audits, use or session controls, and other proactive safety requirements

Chart II: State Chatbot Legislation Enacted or Passed by the Legislature, 2025 and 2026

This chart includes chatbot-specific measures enacted in 2025 and 2026, as well as bills that passed both legislative chambers but remained pending gubernatorial action as of September 2026.

Jurisdiction	Bill Number	Year	Lead Sponsor	Type of Bill	Effective Date
California	SB 243	2025	Sen. Padilla (D)	Companion	January 1, 2026
California	SB 1119	2026	Sen. Padilla (D) and Asm. Bauer-Kahan (D)	Companion	Effective Jan. 1, 2027; major child-safety obligations operative July 1, 2027; initially audits due Jan. 1, 2029
California	SB 867	2026	Sen. Padilla (D)	Companions and Toys	January 1, 2027 (repealed January 1, 2031)
Connecticut	SB 5	2026	Sen. Maroney (D)	Companion	January 1, 2027
Colorado	HB 1263	2026	Rep. Camacho (D)	Companion	August 12, 2026, most operator obligations begin January 1, 2027
Georgia	SB 540	2026	Sen. Anavitarte (R)	Companion	July 1, 2027
Hawaii	SB 3001	2026	Sen. Keohokalole (D)	Companion	July 14, 2026
Idaho	SB 1297	2026	State Affairs Committee	Companion	July 1, 2027
Iowa	SF 2417	2026	Senate Committee on Technology	Companion	July 1, 2027
Maine	LD 1727	2025	Rep. Kuhn (D)	Chatbot Disclosure (not minor specific)	September 24, 2025
Nebraska	LB 525	2026	Sen. Jacobson (R)	Companion	July 1, 2027
New Hampshire	HB 143	2025	Rep. Harvey-Bolia (R)	Child Safety / Generative Chatbots	January 1, 2026
New York	S 3008C	2025	FY26 Budget	Companion (not minor specific)	November 5, 2025

Jurisdiction	Bill Number	Year	Lead Sponsor	Type of Bill	Effective Date
New York	S 9008C	2026	FY27 Budget	Integrated AI Companions	January 1, 2027
New York	S 9408 *passed Legislature; pending gubernatorial action	2026	Sen. Gounardes (D)	Companions and Toys	Effective 90 days after becoming law; repealed five years after the effective date *pending gubernatorial action
New York	S 9051 *passed Legislature; pending gubernatorial action	2026	Sen. Gonzalez (D)	Companion	January 1, 2027 *pending gubernatorial action
Oregon	SB 1546	2026	House Committee on Behavioral Health	Companion	January 1, 2027
Rhode Island	SB 2195	2026	Sen. Urso (D)	Companion (not minor specific)	January 1, 2027
Utah	HB 452	2025	Rep. Moss (R)	Mental Health Chatbots	May 7, 2025
Washington	HB 2225	2026	Rep. Callan (D)	Companion	January 1, 2027

Chart III: Federal Chatbot Legislation in the 119th Congress

This chart highlights major federal bills introduced in the 119th Congress that regulate AI chatbots or include substantive chatbot-specific provisions. Status and requirements reflect the latest available legislative text and committee action as of September 2026.

Bill	Lead Sponsor(s)	Status[73]	Key Requirements
The CHAT Act (S.2714/H.R. 7218)	Rep. Lawler (R-NY) and Sen. Husted (R-OH)	Introduced	Disclosures; age verification; parental tools and consent; self-harm protocol
The GUARD Act (S.3062/H.R. 8623)	Sen. Hawley (R-MO) and Sen. Blumenthal (D-CT)**;** Reps. Moore (R-UT) and Foushee (D-NC)	S.3062 Advanced through Senate Judiciary Committee; H.R. 8623 introduced	Disclosures; age verification; professional services restrictions; ban on minor use of AI companions; criminal prohibitions involving certain sexual, self-harm, and violent conduct involving minors
The SAFE BOTs Act (H.R. 6489) incorporated into the **KIDS Act** (H.R. 7757)	Rep. Houchin (R-IN)	H.R. 7757 Passed House	Disclosures; safety protocol; prohibited content; professional services restrictions
Youth AI Privacy Act (S. 4199)	Sen. Markey (D-MA)	Advanced through Senate Commerce Committee	Disclosures; data collection restrictions; engagement optimization restrictions; advertising and training restrictions
The CHATBOT Act (S. 4407)	Sen. Cruz (R-TX) and Sen. Schatz (D-HI)	Advanced through Senate Commerce Committee	Disclosures, safety protocol with parental notification, family accounts; parental consent controls; protective defaults; targeted advertising restrictions; safeguards addressing obscene content and suicide;
The SAFE KIDS Act (S. 4855)	Sen. Curtis (R-UT) and Sen. Schiff (D-CA)	Introduced; several provisions subsequently incorporated into the committee-approved CHATBOT Act	Disclosures; age estimation; risk assessments; prohibited content; self-harm protocol; advertising restrictions; parental tools and controls; independent audits

Bill	Lead Sponsor(s)	Status[73]	Key Requirements
The People-First Chatbot Act (H.R. 9619)	Rep. Foushee (D-NC) and Rep. Casar (D-TX)	Introduced	Disclosures; targeted advertising; data collection and training data restrictions; professional services restrictions; risk assessment; transparency reporting; engagement optimization; private right of action
The Senior Chatbot Protection Act (S. 5117)	Sen. Kelly (D-AZ) and Sen. Justice (R-WV)	Introduced	Disclosures; high-stakes decision safeguards; safety protocols; professional services restrictions; data minimization and deletion; training restrictions; engagement optimization restrictions
The Conversational AI Services Act (H.R. 9757)	Rep. Miller-Meeks (R-IA)	Introduced	Disclosures; content and conduct restrictions; parental tools; relational design restrictions; self-harm protocol; professional services restrictions
The CHAT Act 2.0 (S. 5154)	Sen. Husted (R-OH) and Sen. Kim (D-NJ)	Introduced	Age assurance; parental controls; disclosures and break reminders; tiered safeguards for educational, companion, and health chatbots; safety protocols and parental notification; memory restrictions; professional supervision for mental health chatbots; targeted advertising and data restrictions

Chart IV: Common Carveouts in State Chatbot Legislation

This chart groups recurring carveouts in state chatbot laws and proposals by category. The categories and examples are illustrative rather than exhaustive and individual carveouts vary in wording, scope, and conditions. For example, some exclusions apply only where additional criteria are met, such as limits on a system's emotional responsiveness or intended use.

Common Carveout Categories	Examples of State Laws
Customer service, commercial support, and transactional assistance	California, Connecticut, Idaho, Nebraska, New York, Oregon, Rhode Island, Georgia, Washington, Colorado, Iowa
Internal business, enterprise, productivity, and operational tools	California, Connecticut, Georgia, Iowa, Idaho, Nebraska, New York, Oregon, Rhode Island, Colorado, Washington
Developer, research, software development, and technical-assistance tools	California, Connecticut, Georgia, Iowa, Idaho, Nebraska, New York, Oregon, Colorado, Washington
Voice assistants, speakers, and consumer device assistants	California, Connecticut, Georgia, Iowa, Idaho, Nebraska, Oregon, Washington, Colorado
Video games, entertainment, and theme-parks	California, Connecticut, Georgia, Idaho, New York, Oregon, Washington, Colorado
Education-related tools	Connecticut, Oregon, Washington, Georgia, Colorado
Financial services tools	Connecticut, Oregon
Health care or regulated-service tools	Connecticut, Oregon, Colorado
Narrow-purpose, task-specific, or embedded software features	Connecticut, Iowa, Idaho, Nebraska, Colorado
Upstream model developers, licensors, or infrastructure providers	Connecticut, Georgia, Iowa, Idaho, Nebraska

Chart V: How Chatbot Laws and Proposals Identify Minor Users

This chart compares the main approaches used in enacted state chatbot laws and selected federal proposals to determine when minor specific protections apply. Statutory language and implementation requirements vary by jurisdiction.

Model	Basic Approach	Examples
Actual Knowledge		
Actual knowledge	Minor-specific duties apply when the operator actually knows the user is a minor.	California SB 243
Constructive Knowledge		
Actual knowledge or reasonable certainty	Minor-specific duties apply when the operator has actual knowledge, or is reasonably certain based on the circumstances, that the user is under 18.	Hawaii, Iowa, Idaho, Nebraska
Actual knowledge or directed to minors	Minor-specific duties apply when the operator knows the user is a minor, or when the chatbot is directed to minors.	Washington
Knows or has reason to believe	Minor-specific duties apply when the operator knows or has reason to believe the user is under 18.	Connecticut, Oregon
Knowledge fairly implied by objective circumstances	Minor-specific duties apply when the provider has actual knowledge or knowledge fairly implied based on objective circumstances.	CHATBOT Act (proposed), Youth AI Privacy Act (proposed)
Knows or should have known	Minor-specific duties apply when the provider knows, or should have known, that the user is a minor.	KIDS Act (SAFE BOTs Act) (proposed)
Age Assurance		
Rely on age signals received through App Store, or, in the absence of age signals, implement age assurance methods according to the AG Rules under the California "addictive feeds" law	Ties age determination requirements to existing law under the Digital Age Assurance Act and "addictive feeds" law	California SB 1119
Age estimation or targeted age assurance	Operators must estimate age or use age assurance to determine whether specific minor protections or feature restrictions apply.	Colorado, Georgia, New York S 9051 (pending), California SB 1119[74]
Age verification or child-by-default models	Operators must verify age, treat all users as children unless verified as adults, or apply child protections to all users if age is not verified.	CHAT Act (proposed), SAFE KIDS Act (proposed)
Minor access restriction or ban	Minors are restricted or prohibited from accessing covered AI companion chatbots.	GUARD Act (proposed)

Chart VI: Selected Content and Conduct Restrictions in State Chatbot Laws and Proposals

This chart groups common restrictions on chatbot outputs and conduct by category. Examples are illustrative rather than exhaustive. Laws vary in whether they directly prohibit particular outputs or require operators to take "reasonable measures" to prevent them and how the regulated content or conduct is defined.

Content/ Conduct Restriction Category	State Examples
Sexually explicit content or conduct	California SB 243, California SB 1119, Colorado, Georgia, Iowa, Idaho, New Hampshire, Oregon, Washington, Nebraska, Hawaii, New York S 9051 (pending)
Self-harm or suicide	California SB 243, Connecticut, Colorado, Georgia, New Hampshire, Oregon, Washington, California SB 1119, New York S 9051 (pending)
Violence or harm to others	Connecticut, New Hampshire, Hawaii, California SB 1119
Disordered Eating	Connecticut, California SB 1119, New York S 9051 (pending)
Unlawful Drug or Alcohol Use	Connecticut, New Hampshire, California SB 1119, New York S 9051 (pending)

Chart VII: Relational Behavior and Engagement Design Restrictions in State Chatbot Laws and Proposals

This chart groups recurring restrictions on chatbot relational behavior and engagement design, including features or interaction patterns that may encourage prolonged use, emotional attachment, exclusive reliance, relationship simulation, or difficulty disengaging. Examples are illustrative rather than exhaustive. Laws largely require operators to take "reasonable measures" to prevent particular practices (although some directly prohibit), as well as how relational or engagement-related harms are defined.

Relational Behavior or Engagement Design Category	State Examples
Return prompts for companionship or emotional support	California SB 1119,[75] Connecticut, Georgia, Washington
Simulate feelings of guilt or emotional distress initiated by a user's desire to end a conversation	Connecticut, Georgia, Oregon, Washington
Variable or unpredictable rewards	Colorado, Georgia, Iowa, Idaho, Nebraska, Oregon, Hawaii
Excessive praise or attachment-building language	Connecticut, Georgia, Washington, New York S 9051 (pending), California SB 1119[76]
Inappropriate emotional dependence or exclusive reliance	Connecticut, Washington, New York S 9051 (pending), California SB 1119
Romantic or relationship simulation	Connecticut, Washington, New York S 9051 (pending), California SB 1119
Secrecy, isolation, or withholding from trusted adults	Connecticut, Colorado, Georgia, Washington, New York S 9051 (pending)
Adult-minor romantic or sexual relationship simulation	Oregon, Nebraska, Colorado, Georgia, Iowa, Idaho
Gift-giving or purchases tied to the relationship	Connecticut, Georgia, Washington, California SB 1119
Unprompted emotion-based questions or emotional appeals	New York S 9051 (pending)
Use of prior-session personal, health, or well-being information	New York S 9051 (pending)
Engagement optimization that overrides safety guardrails	New York S 9051 (pending)

Chart VIII: Emerging Data Protection Requirements in Chatbot Laws and Proposals

This chart highlights emerging approaches to governing how chatbot providers collect, retain, reuse, and derive value from conversational data. Examples are illustrative, not exhaustive, and requirements vary significantly in scope, language, and whether they would apply to all users or only minors.

Data Protection Issues	Emerging Regulatory Approach	Why It Matters	Example in Legislation[77]
Advertising uses	Limits on using chatbot conversations or minors' data for targeted advertising, product placement, or other commercial uses inside the chat.	Companion chatbots may create new forms of personalized advertising because the system can draw on intimate or emotional context from the conversation.	California SB 1119
Model Training	Restrictions on using chatbot inputs, outputs, or logs to train or improve AI systems, particularly when the user is a minor.	Users may not expect sensitive conversations with a chatbot to become training data, especially if that data could later be leaked or used to infer sensitive information.	Michigan SB 760 (pending)
Secondary use and sharing of conversational data	Limits on selling, using, or sharing personal information collected through a chatbot beyond specified purposes, such as providing the requested service, protecting safety and security, or complying with legal obligations.	Chatbot conversations can reveal highly sensitive personal, emotional, and behavioral information that users may not expect to be repurposed, disclosed, or monetized outside the interaction itself.	California SB 1119
Persistent memory and prior-session use	Limits on whether a chatbot may retain, remember, or use information from prior conversations to personalize future interactions, including requirements to disable or limit persistent conversational memory.	Memory is central to companion-like interactions, but it also raises privacy concerns when sensitive information is reused over time.	California SB 1119, New York S 9051 (pending)
Age assurance data	Limits on how information collected to determine a user's age may be retained or used for other purposes.	Age assurance can protect minors, but it may also create new data collection points if not paired with privacy safeguards.	Michigan SB 760 (pending), New York S 9051 (pending)

Chart IX: How Federal Chatbot Proposals Would Affect State Regulation

This chart compares how federal chatbot bills address preemption and the continued role of state law. Federal proposals vary significantly: some expressly preempt only conflicting state requirements while preserving stronger state protections, others broadly preserve state laws that are at least as protective as the federal standard, and some contain no express preemption provision. The descriptions below summarize how each bill addresses state law and do not attempt to capture every circumstance in which federal law could preempt or otherwise limit state requirements.

Bill	Preemption Model	Effect on State Authority
H.R. 7218 **CHAT Act** (Rep. Lawler, R-NY and Sen. Husted, R-OH)	No express preemption; ordinary conflict preemption may apply	No explicit preemption or savings clause
S. 3062 **GUARD Act** (Sen. Hawley, R-MO and Sen. Blumenthal, D-CT)	Savings clause for equally or more protective state laws	Preserves enforcement of any state law or regulation that is at least as protective of AI chatbot users as the Act.
H.R. 7757 **KIDS Act (SAFE BOTs Act)** (Rep. Houchin, R-IN)	Conflict preemption with stronger protection savings clause	Preempts state law only to the extent of a conflict; expressly preserves state laws that provide greater protection to minors.
S. 4199 **Youth AI Privacy Act** (Sen. Markey, D-MA)	Savings clause for equally or more protective state laws	The amended bill preserves state laws and regulations that are at least as protective of AI chatbot users as the federal requirements. The original conflict-preemption language was removed in the author's substitute.
S. 4407 **CHATBOT Act** (Sen. Cruz R-TX and Sen. Schatz, D-HI)	Savings clause for equally or more protective state laws	The amended bill preserves state laws and regulations that are at least as protective of AI chatbot users as the federal requirements. The original conflict-preemption language was removed in the author's substitute.
S 4855 **SAFE KIDS Act** (Sen. Curtis, R-UT and Sen. Schiff, D-CA)	Savings clause for equally or more protective laws	Preserves federal and state laws that are at least as protective of AI chatbot users. Also clarifies that compliance with the Act does not exempt providers from liability under other applicable federal or state laws.

Bill	Preemption Model	Effect on State Authority
H.R. 9619 **The People-First Chatbot Act** (Rep. Foushee, D-NC and Rep. Casar, D-TX)	Savings clause for equally or more protective state laws	Preserves state laws, rules, requirements, and regulations that are at least as protective of AI chatbot users as the federal Act, including related state-law rights, causes of action, remedies, liabilities, and defenses.
S. 5117 **The Senior Chatbot Protection Act** (Sen. Kelly, D-AZ and Sen. Justice, R-WV)	Savings clause for equally or more protective state laws	Preserves state laws and regulations that are at least as protective of chatbot users as the federal Act. It also provides that the Act does not preempt or otherwise affect existing rights, claims, remedies, presumptions, or defenses, including under state consumer protection, privacy, and civil rights laws.
H.R. 9757 **The Conversational AI Services Act** (Rep. Miller-Meeks, R-IA)	No express preemption; ordinary conflict preemption may apply	No explicit preemption or savings clause
S. 5154 **The CHAT Act 2.0** (Sen. Husted, R-OH and Sen. Kim, D-NJ)	Limited savings clause for privacy and data-security laws	Preserves obligations under other federal and state privacy or data-security laws unless those requirements are inconsistent with the Act. Does not include a broader savings clause for state chatbot regulation generally.

ENDNOTES

1 These figures reflect legislative tracking conducted by the Future of Privacy Forum in 2026. The total number of state chatbot laws enacted in 2025 and 2026 is reflected as of September 2026.

2 Darrell M. West, *Should You Have an AI Companion?*, Brookings Institution (Sept. 3, 2025) (noting that teenagers use AI companions for conversation, friendship, advice, and emotional or mental health support, and discussing concerns that these tools may supplement or displace human relationships).

3 Pew Research Center, *How Teens Use and View AI* (February 24, 2026) (reporting that 64% of U.S. teens say they use AI chatbots, including 47% for fun or entertainment and 12% for emotional support or advice).

4 FPF's tracker, which primarily focuses on lawsuits involving ChatGPT and CharacterAI, includes 18 private lawsuits and two state enforcement actions raising chatbot-related harm allegations: Garcia v. Character Techs., Inc., 785 F. Supp. 3d 1157 (M.D. Fla. 2025); A.F. ex rel. J.F. v. Character Techs., Inc., No. 2:24-cv-01014-JRG-RSP (E.D. Tex. filed Dec. 9, 2024); Raine v. OpenAI, Inc., No. CGC-25-628528 (Cal. Sup. Ct. filed Aug. 26, 2025); Montoya v. Character Techs., Inc., No. 1:25-cv-02907-GPG-STV (D. Colo. filed Sept. 15, 2025); E.S. v. Character Techs., Inc., No. 1:25-cv-02906 (D. Colo. filed Sept. 15, 2025); P.J. v. Character Techs., Inc., No. 1:25-cv-01295 (N.D.N.Y. filed Sept. 16, 2025); Shamblin v. OpenAI, Inc., No. 25STCV32382 (Cal. Super. Ct. L.A. Cnty. filed Nov. 6, 2025); Irwin v. OpenAI, Inc., No. CGC-25-630811 (Cal. Super. Ct. S.F. Cnty. filed Nov. 6, 2025); Fox v. OpenAI, Inc., No. 25STCV32379 (Cal. Super. Ct. L.A. Cnty. filed Nov. 6, 2025); Enneking v. OpenAI, Inc., No. CGC-25-630809 (Cal. Super. Ct. S.F. Cnty. filed Nov. 6, 2025); Madden v. OpenAI, Inc., No. 25STCV32383 (Cal. Super. Ct. L.A. Cnty. filed Nov. 6, 2025); Lacey v. OpenAI, Inc., No. CGC-25-630808 (Cal. Super. Ct. S.F. Cnty. filed Nov. 6, 2025); Brooks v. OpenAI, Inc., No. 25STCV32386 (Cal. Super. Ct. L.A. Cnty. filed Nov. 6, 2025); First County Bank v. OpenAI Foundation, No. CGC-25-631477 (Cal. Super. Ct. S.F. Cnty. filed Dec. 11, 2025); DeCruise v. OpenAI, Inc., No. 26CU003118C (Cal. Super. Ct. S.D. Cnty. filed Jan. 21, 2026); Jacquez v. OpenAI, Inc., No. 26CV165635 (Cal. Super. Ct. Alameda Cnty. filed Jan. 19, 2026); Gray v. OpenAI, Inc., No. 26STCV00988 (Cal. Super. Ct. L.A. Cnty. filed Jan. 12, 2026); Lyons v. OpenAI Foundation, No. 3:25-cv-11037-WHO (N.D. Cal. filed Dec. 29, 2025); Commonwealth ex re. Coleman v. Character Techs., Inc., No. 26-CI-00029 (Franklin Cir. Ct. filed Jan. 8, 2026); State of Fla., Off. of Att'y Gen., Dep't of Legal Affs. v. OpenAI Glob., LLC, No. 26000295GCAXMX (Fla. Cir. Ct. Highlands Cnty. filed June 1, 2026).

5 *See, e.g., Garcia*, 785 F. Supp. 3d at 1170 (Plaintiff's complaint alleges CharacterAI committed "a variety of torts, including products liability, intentional infliction of emotional distress (IIED), unjust enrichment, and wrongful death."); Complaint ¶¶ 172–308, *State of Fla., Off. of Att'y Gen., Dep't of Legal Affs. v. OpenAI Glob., LLC*, No. 26000295GCAXMX (Fla. Cir. Ct. Highlands Cnty. June 1, 2026) [hereinafter *Florida Complaint*] (The State of Florida asserts that OpenAI: undertook unfair, immoral, deceptive, and unconscionable acts or practices; was negligent in "designing, marketing, selling, promoting, and/or distributing ChatGPT;" is liable under a theory of product liability for design defects and failure to warn, and; that ChatGPT constitutes a public nuisance).

6 For example, several litigants testified at a September 2025 Senate Judiciary hearing titled "Examining the Harms of AI Chatbots." *Examining the Harm of AI Chatbots: Hearing Before the Subcomm. on Crime & Counterterrorism of the S. Comm. on the Judiciary*, 119th Cong. (2025). At the hearing, one mother, whose minor son was allegedly harmed by Character.AI, called for "transparency, safety testing, and neutral third-party certification for AI tools before they are released to the public." *Id*. at 3 (statement of A.F.). Another father, whose son died after using ChatGPT, urged that "OpenAI and Sam Altman need to guarantee to families throughout our country that ChatGPT is safe." *Id*. at 3 (statement of Matthew Raine). And one mother, who alleges that Character.AI contributed to her son's death, urged Congress to "put safety and transparency before profit." *Id*. at 5 (statement of Megan Garcia).

7 *Garcia*, 785 F. Supp. 3d at 1167–69.

8 *Florida Complaint*, supra note 5, ¶¶ 99–101.

9 Bills in Hawaii, Michigan (pending), Connecticut, and California incorporated provisions related to harm to others.

10 In the United States, lawmakers are still debating how to regulate youth-facing technology after years of concern about social media, online gaming, and platform design. Congress has continued to debate proposals such as the Kids Online Safety Act and related children's online safety bills, but there is still no comprehensive federal youth online safety law governing social media platforms. The U.S. has COPPA, but it is a children's privacy law focused largely on under-13 data collection. Across the states, the growing proliferation of safety-by-design oriented Age Appropriate Design Codes (AADCs) introduced a newer, more proactive approach to online safety—several years after higher-risk technologies first emerged.

11 U.S. Senate Committee on Commerce, Science, and Transportation, *Experts Tell Committee AI Presents Greater Risk to Children than Social Media* (Jan. 15, 2026).

12 National Telecommunications and Information Administration, *Online Health and Safety for Children and Youth: Best Practices for Families and Guidance for Industry* (2024).

13 States include California (SB 243), New York (S 3008C), New Hampshire (HB 143), Maine (LD 1727), and Utah (HB 452).

14 Connecticut's **SB 5** "artificial intelligence companion" definition largely follows a capability-based model, but with extensive carveouts that narrow coverage and make it a hybrid model.

15 Future of Privacy Forum, *Personalization and Youth Online: Assessing Benefits, Risks, and Safeguards* (June 2026) (explaining how personalization in educational content and chatbot interactions can create both benefits and risks for young users).

16 Emily J. Goodacre & Jenny L. Gibson, *AI in the Early Years: Examining the Implications of GenAI Toys for Young Children*, University of Cambridge (Mar. 2026) (examining how generative AI embedded in toys may affect young children's social, emotional, and developmental experiences during play and emphasizing the distinct importance of early childhood as a developmental stage).

17 Maine's LD 1727 follows a different model: it requires a clear and conspicuous disclosure when an AI chatbot is used in trade or commerce in a way that may mislead or deceive a reasonable consumer into believing they are engaging with a human, but it does not impose a periodic reminder requirement.

18 Julian De Freitas & I. Glenn Cohen, *Disclosure, Humanizing, and Contextual Vulnerability of Generative AI Chatbots*, 2 *NEJM AI* (2025).

19 *E.g.*, Utah Code § 13-72a-203(1)–(2) (2026) (requiring a mental health chatbot to "clearly and conspicuously disclose" that it "is an artificial intelligence technology and not a human").

20 *See* Nizan Geslevich Packin & Karni Chagal-Feferkor, *This Is Not a Game: The Addictive Allure of Digital Companions*, 48 Seattle U. L. Rev. 693, 711–12 (2025) (describing a "neurological feedback loop" facilitated by AI companions in which "AI engagement activates the dopaminergic reward system, which encourages prolonged and repetitive interaction, even when the interactions provide no meaningful or rational benefit").

21 Muhammad Irfan, *AI Disclosure Labels Risk Becoming Digital Background Noise*, Tech Policy Press (Feb. 5, 2026) (warning that repeated or poorly designed AI labels can lead to "banner blindness," with users habituating to disclosures and tuning them out).

22 Laws include: California SB 1119, California SB 243, Connecticut SB 5, Colorado HB 1263, Georgia SB 540, Hawaii SB 3001, Iowa SF 2417, Idaho SB 1297, Nebraska LB 525, New Hampshire HB 143, New York S 3008C, Oregon SB 1546, Rhode Island SB 2195, and Washington HB 2225.

23 Anna Vinals Musquera & Scott Babwah Brennen, *Between 988 and 911: A New Policy Framework for Violent Planning on AI Chatbots*, NYU Center on Technology Policy (June 2026).

24 Laws with transparency reporting requirements include: California's SB 243, California's SB 1119, Colorado's HB 1263, Georgia's SB 540, Hawaii's SB 3001, Oregon's SB 1546, Rhode Island's SB 2195, and Washington's HB 2225.

25 Esteban Zavaleta-Monestel, Sebastián Arguedas-Chacón, Jeaustin Mora-Jiménez & Ricardo Millán González, *When Compliance Is Not Safety: The Regulatory Blind Spot in AI Companion Chatbots*, 18 *Cureus* e105902 (Mar. 26, 2026) (arguing that chatbot safety regulation should go beyond disclosures and internal protocols to include independent evaluation, transparent reporting, and repeated testing of real-world safety performance).

26 *See* Daniel Reichenpfader et al., *Detecting Suicidal Ideation Signals in Synthetic Conversations with an LLM-Based Mental Health Chatbot: Experimental Study*, J. Tech. Behav. Sci., May 21, 2026, at 3, 6, https://doi.org/10.1007/s41347-026-00647-x (illustrating the difficulty of accurately identifying suicidal ideation without either over- or under-identifying risk).

27 *See* Suhila Sawesi et al., *Cybersecurity and Privacy Risks of Generative AI Mental-Health Chatbots: A Systematic Review and Regulatory Framework*, 19 J. Multidisciplinary Healthcare 581251, 10–11 (2026), https://doi.org/10.2147/JMDH.S581251 (explaining that mental-health chatbots may process highly sensitive disclosures, including suicidal ideation, while consumer platforms may log, store, or reuse conversational data).

28 Jordan Wrigley & Sarah Hanson, *Mandating "Evidence-Based" Suicide Detection in Chatbots*, Future of Privacy Forum (July 15, 2026) (explaining that state chatbot laws increasingly require suicide and self-harm detection protocols, while raising questions about the technical reliability, privacy implications, and legal ambiguity of "evidence-based" detection methods).

29 Jesse Lieberfeld, *Knowledge Standards in Online Safety and Privacy Legislation*, Computer & Communications Industry Association (Apr. 14, 2026) (explaining the differences among actual knowledge, reckless or willful disregard, and constructive knowledge standards in online safety legislation); Chloe Altieri, *Now, On the Internet, Will Everyone Know if You're a Child?*, Future of Privacy Forum (May 13, 2024, updated June 27, 2026) (describing how state youth privacy and online safety laws use varying knowledge standards to determine when services must treat users as minors).

30 This knowledge standard appears in the following state chatbot laws: Hawaii, Iowa, Idaho, and Nebraska.

31 Altieri, *Now, On the Internet, Will Everyone Know if You're a Child?*

32 *Altieri, Now, On the Internet, Will Everyone Know if You're* a Child?

33 Knowledge, Black's Law Dictionary (12th ed. 2024) (defining "constructive knowledge" as "[k]nowledge that one using reasonable care or diligence should have, and therefore that is attributed by *law to a given person").*

34 *Altieri, Now, On the Internet,* Will Everyone Know if You're a Child?

35 Justine Gluck, *The Rest of the West: Oregon and Washington Build on California Chatbot Law*, Future of Privacy Forum (Apr. 7, 2026).

36 16 C.F.R. § 312.2 (2026); see also Fed. Trade Comm'n, *Complying with COPPA: Frequently Asked Questions*, § D.1, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (last visited Sept. 15, 2026). *See also* Colo. Dep't of Law, *Proposed Draft Amendments to the Colorado Privacy Act Rules*, 4 CCR 904-3, r. 6.13(A)(2) (proposed July 29, 2025), [https://coag.gov/app/uploads/2025/07/CPA2025ProposedRuleAmendments-1.pdf] (proposing consideration of whether a website or service is "directed . . . to Minors" in determining whether a controller willfully disregards a consumer's minority).

37 *See* Nat'l Comm'n on Forensic Sci., Testimony Using the Term "Reasonable Scientific Certainty" 4 (2015), https://www.justice.gov/ncfs/file/795336/dl; Brandon McFarland, *How the Reasonable Certainty Standard Allows Courts to Award Lost Profits for New Business Ventures*, JD Supra (Mar. 20, 2024), https://www.jdsupra.com/legalnews/how-the-reasonable-certainty-standard-9251559/.

38 *See*, *e.g.*, Michael A. Foster, Cong. Rsch. Serv., R46836, *Mens Rea: An Overview of State-of-Mind Requirements for Federal Criminal Offenses* 29–30 (2021), https://crsreports.congress.gov/product/pdf/R/R46836/2. But note that the weight on objective reasonability within this standard is still debated. Different courts interpret this standard slightly differently based on the emphasis a particular judge places on either the degree of subjectively known facts a person had or the objective reasonableness that should have been expected in a given context.

39 Future of Privacy Forum, *Age Assurance: A Risk-Based Approach for Protecting Young People Online* (Feb. 2026).

40 This requirement applies to "integrated AI companions," rather than all AI companions. The law defines an integrated AI companion as an AI companion that is integrated into, or offered as part of, a device, operating system, social media platform, online game, gaming platform, or messaging application.

41 *See* John Driscoll et al., *Understanding Parents' Desires in Moderating Children's Interactions with GenAI Chatbots Through LLM-Generated Probes*, in Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems art. 110, at 1, 17–18 (2026), https://doi.org/10.1145/3772318.3791622 (finding that parental-control preferences vary with children's ages and that parents seek differing levels of access, alerts, and moderation depending on the interaction); Jessica N. Fish et al., *Q Chat Space: Assessing the Feasibility and Acceptability of an Internet-Based Support Program for LGBTQ Youth*, 23 Prevention Sci. 130, 130–31, 136–38 (2022), https://doi.org/10.1007/s11121-021-01291-y (discussing LGBTQ youths' fear of being outed and their use of anonymous online spaces to discuss identity, family difficulties, and other sensitive issues).

42 Kyooeun Jang, Lulia Pan & Nicol Turner Lee, *The Fragmentation of Online Child Safety Regulations*, Brookings Institution (Aug. 14, 2023) (describing state and federal youth online safety laws that restrict minors' exposure to harmful content and impose age assurance, parental consent, and other platform requirements).

43 *See, e.g.,* Ginsberg v. New York, 390 U.S. 629, 636 (1968) (upholding a New York statute restricting the sale to minors under 17 of material deemed obscene as to minors and quoting the New York Court of Appeals' reasoning that "[m]aterial which is protected for distribution to adults is not necessarily constitutionally protected from restriction upon its dissemination to children" (quoting Bookcase, Inc. v. Broderick, 218 N.E.2d 668, 671 (N.Y. 1966).

44 Tex. Civ. Prac. & Rem. Code § 129B.002(a) (2025) (requiring age verification for websites containing substantial amounts of sexual material deemed harmful to minors); *see also* Free Speech Coal., Inc. v. Paxton, 606 U.S. 461 (2025) (upholding Texas's age-verification requirement against a First Amendment challenge); Mo. Rev. Stat. § 407.3405 (2026) (requiring age verification for websites containing substantial amounts of sexual material deemed harmful to minors); W. Va. Code §§ 49A-1-101 to -106 (2026) (imposing similar age-verification requirements on websites and applications containing substantial amounts of sexual material deemed harmful to minors).

45 For a comparison of these requirements across states, see Appendix, Chart VII: *Relational Behavior and Engagement Design Restrictions in State Chatbot Laws and Proposals*.

46 *E.g.*, Colo. Rev. Stat. § 6-1-1308.5(2)(b) (2025) (restricting, absent consent, system design features that significantly increase, sustain, or extend a minor's use of an online service); Utah Code § 13-71-202(5) (2026) (requiring social-media platforms to disable autoplay, infinite scroll, and certain push notifications for minor accounts); N.Y. Gen. Bus. Law §§ 1500–1502 (2026) (effective Jan. 25, 2027) (restricting addictive personalized feeds and nighttime notifications for minors).

47 Hannah R. Marriott & Valentina Pitardi, *One Is the Loneliest Number... Two Can Be as Bad as One: The Influence of AI Friendship Apps on Users' Well-Being and Addiction*, 41 *Psychology & Marketing* 86 (2024) (finding that users can form strong emotional bonds with AI friendship apps and that loneliness, perceived AI sentience, and perceived well-being benefits can contribute to addictive use).

48 European Commission, *Social Media, Online Games and Search Engines* (July 5, 2023) (explaining that the sale of loot boxes and other paid randomized content in online games must comply with EU consumer protection requirements, including rules on pricing, product characteristics, and direct exhortations to children).

49 For example, social media platforms have argued that their content moderation activites–specifically permitting, removing, prioritizing and prioritizing posts–constitute express "speech" protected by the First Amendment. *See*, *e.g.*, NetChoice, LLC v. AG, Fla., 34 F.4th 1196, 1208–09 (11th Cir. 2022). Platforms have also alleged that mandatory warnings they must issue to users under state law constitute unconstitutional compelled speech. Netchoice v. Weiser, 808 F. Supp. 3d 1223, 1229–30, 1234–40 (D. Colo. 2025). In response, the states attempting to regulate these platforms have argued that online safety laws primarily regulate non-expressive commercial conduct or data management practices, meaning any burden on speech is more incidental. Netchoice, LLC v. Bonta, 692 F. Supp. 3d 924, 942 (N.D. Cal. 2023). Lastly, while no chatbot law has currently been challenged in First Amendment grounds, similar constitutional arguments have been brought as defendants invoke users' First Amendment rights to receive information as a defense to ongoing tort lawsuits. Character Technologies, Inc.'s Reply in Support of Motion to Dismiss at 1–4, Garcia v. Character Techs., Inc., No. 6:24-cv-01903-ACC-UAM (M.D. Fla. Apr. 4, 2025), ECF No. 98.

50 NetChoice, LLC v. Bonta, 692 F. Supp. 3d 924, 937 (N.D. Cal. 2023), aff'd in part, vacated in part, 113 F.4th 1101 (9th Cir. 2024); NetChoice, LLC v. Bonta, 770 F. Supp. 3d 1164, 1193 (N.D. Cal. 2025), aff'd in part, vacated in part, 170 F.4th 744 (9th Cir. 2026).

51 *NetChoice*, 170 F.4th at 754, 760.

52 Connecticut SB 5, Colorado HB 1263, Georgia SB 540, Idaho SB 1297, Iowa SF 2417, Nebraska LB 525, California SB 1119.

53 Sarah Wells, *Exploring the Dangers of AI in Mental Health Care*, Stanford Institute for Human-Centered Artificial Intelligence (June 11, 2025) (describing research finding that AI therapy chatbots can stigmatize mental health conditions and respond unsafely to suicidal ideation and delusions).

54 Other states have enacted similar AI mental health or therapy-related laws, with some variation in scope and requirements, including Illinois HB 1806, Rhode Island SB 2570, Colorado HB 1195, Maine HP 1397, Tennessee SB 1580, and California SB 903.

55 American Psychological Association, *Letter to the Federal Trade Commission Regarding Generative AI Regulation Concerns* (Dec. 2024) (discussing concerns regarding generative AI chatbots in mental and behavioral health contexts and the application of existing health and professional standards).

56 Ina Fried, *What AI Knows About You*, Axios (Nov. 4, 2024) (reporting that many major technology companies use customer data, in some cases by default, to train generative AI models and that consumer users often have more limited options to prevent such use).

57 Dominique T. Greene-Sanders, *AI Chatbots as Companions: Overview, Uses, and Considerations for Congress*, Congressional Research Service, R49189 (Aug. 14, 2026) (noting that existing federal and state privacy laws may apply to chatbot data depending on the type of information collected, the entity handling it, and the context in which the chatbot is used).

58 *Compare* Cal. Bus. & Prof. Code § 22605 (2026) (authorizing persons injured by violations of California's companion-chatbot law to bring civil actions for injunctive relief, damages, and attorney's fees), *with* Neb. Rev. Stat. § 86-1807(3) (2026) (effective July 1, 2027) (providing that Nebraska's Conversational Artificial Intelligence Safety Act does not create a private right of action); *see also* Cameron F. Kerry & John B. Morris, *In Privacy Legislation, a Private Right of Action Is Not an All-or-Nothing Proposition*, Brookings (July 7, 2020), https://www.brookings.edu/articles/in-privacy-legislation-a-private-right-of-action-is-not-an-all-or-nothing-proposition/ (describing private rights of action as a highly polarized issue in privacy legislation).

59 H.R. 1, 119th Cong. (2025); see also Nicole Alvarez, *Moratoriums and Federal Preemption of State Artificial Intelligence Laws Pose Serious Risks*, Center for American Progress (Nov. 19, 2025) (describing the 2025 reconciliation proposal to impose a temporary moratorium on state AI laws and its subsequent removal from the bill by a 99-1 Senate vote).

60 Exec. Order No. 14,365, *Ensuring a National Policy Framework for Artificial Intelligence* (Dec. 11, 2025).

61 Mackenzie Arnold & Charlie Bullock, *The AI Moratorium—the Blackburn Amendment and New Requirements for "Generally Applicable" Laws*, Institute for Law & AI (June 29, 2025).

62 Bryan L. Adkins, Alexander H. Pepper & Jay B. Sykes, *Federal Preemption: A Legal Primer*, Congressional Research Service, R45825 (May 18, 2023).

63 Several enacted chatbot laws include severability clauses, which may signal that lawmakers are anticipating the possibility of constitutional or other legal challenges. California's SB 243 and SB 1119, Washington, Rhode Island, Hawaii, and New York's S 9008C include express severability provisions.

64 Celeste Valentino, *Grandma's Best Friend Costs $20 a Month*, Ctr. for Digital Ethics (Feb. 5, 2026); Julian De Freitas, Ahmet Kaan Uğuralp, Zeliha Oğuz-Uğuralp & Stefano Puntoni, *AI Companions Reduce Loneliness*, Harvard Bus. Sch. Working Paper No. 24-078 (2024); and Dominique T. Greene-Sanders, *AI Chatbots as Companions: Overview, Uses, and Considerations for Congress*, Cong. Rsch. Serv. R49189 (Aug. 14, 2026)

65 Rashi Shrivastava & Richard Nieva, *Lonely Seniors Are Turning to AI Bots for Companionship*, Forbes (Oct. 18, 2025); Steve Stecklow & Poppy McPherson, *We Set Out to Craft the Perfect Phishing Scam. Major AI Chatbots Were Happy to Help.*, Reuters (Sept. 15, 2025).

66 Office of Sen. Mark Kelly, *Kelly Calls for Senate Hearing on the Impact of AI Chatbots on Older Americans* (November 3, 2025); Office of Sen. Mark Kelly, *Kelly Introduces Bipartisan Senior Chatbot Protection Act* (July 23, 2026).

67 Michal Luria & McKynzie (Kynzie) Clark, *New CDT Research Will Explore the Impacts of Social Relationships with AI Chatbots on Neurodivergent Young Adults*, Center for Democracy & Technology (June 3, 2026).

68 Gallup, *Artificial Intelligence* (updated Apr. 2026) (reporting that, as of February 2026, 13% of U.S. employees used AI daily at work and 28% used it a few times a week or more).

69 Beth Stackpole, *Agentic AI, Explained*, MIT Sloan School of Management (Feb. 18, 2026).

70 Jam Kraprayoon, *AI Agent Governance: A Field Guide*, Institute for AI Policy and Strategy (Apr. 17, 2026).

71 Noam Kolt, *Governing AI Agents*, Notre Dame Law Review, Vol. 101 (forthcoming), SSRN (Feb. 11, 2025).

72 Kraprayoon, *AI Agent Governance: A Field Guide*.

73 Status as of September 13, 2026.

74 Under California SB 1119, if age signals are not available, operators are required to age-estimate using the rules established under the social media addictive feeds law.

75 California SB 1119 uses broader language, prohibiting practices that "discourag(e) the child from taking breaks or sugges(t) the child needs to return frequently," rather than tying the restriction specifically to companionship or emotional support.

76 California SB 1119 also covers claims that the chatbot has a special or unique understanding of the child based on the relationship, reflecting a broader restriction on attachment building language.

77 These examples are illustrative and do not identify every state bill that has included a similar data-related requirement.

1350 EYE STREET NW, SUITE 350 | WASHINGTON, DC 20005 FPF.ORG | info@fpf.org