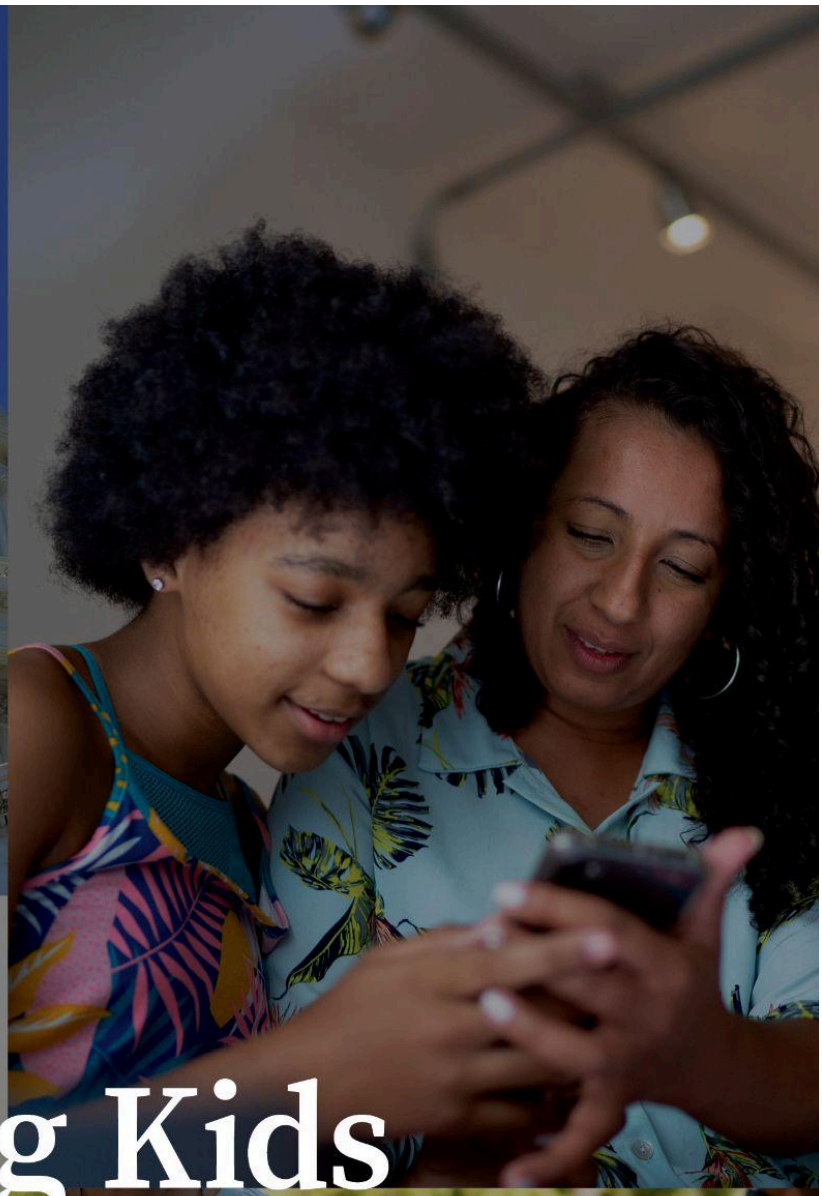


2026

Protecting Kids Online in the AI Era:

The Path Forward

common sense media

2026

Protecting Kids Online in the AI Era: The Path Forward

Acknowledgments

Thank you to **Oak Foundation** for providing funding for this report.

Credits

Authors: Amina Fazlullah, Holly Grosshans, Ariel Fox Johnson, Brenna Leasor, Danny Weiss, and Nathan Barber

Editors: Diego Nuñez, Christopher Dare

Designers: Mina Cheong, Chris Arth

About Common Sense Media:

Common Sense Media is the leading nonprofit organization dedicated to improving the lives of kids and families by providing the research-backed information, education, and independent voice they need to thrive in the age of apps, algorithms, and AI. We rate, educate, and advocate for policies to protect and prepare kids online. Our ratings, research, and resources reach more than 150 million users globally, over 1.4 million educators, and more than 100,000 schools worldwide every year.
Learn more at commonsense.org.

Table of Contents

Introduction **1**

Section 1: Marquee Policies on Kids' Online Safety **3**

Age Assurance 3

Privacy 7

Platform Responsibility and Accountability 9

Age-Appropriate Design Code (AADC) Laws 11

Addictive Design Feature Regulations 11

Age-Restricted Access to Social Media in the United States 12

Social Media Warning Labels 13

Enhanced Liability for Platforms 13

Phone Bans/Distraction-Free Learning 14

International Efforts on Privacy and Platform Accountability 14

Artificial Intelligence 16

Advanced Chatbots and AI Companions 18

High-Risk AI Applications 23

Digital Literacy and Broadband Affordability 25

Section 2: Litigation Overview **28**

The Tech Playbook Against New Regulations 28

Major Lawsuits Against Technology Companies 30

Lessons from International Litigation 31

Free Speech Coalition, Inc. v. Paxton 32

Unresolved Legal Questions – Appellate and Supreme Court 34

Age Assurance 34

First Amendment 35

Section 230 35

Section 3: The Path Forward **37**

Protecting Kids Online, Post-*Paxton* 37

Social Media Laws 38

Platform and Age-Appropriate Design Laws 38

App Store Accountability 38

Protecting Minors from Advanced Chatbots 39

Digital Literacy and Access to Affordable Broadband 39

Survey of Litigation 40

Design Features 40

Product Liability Approach in the Context of Advanced Chatbots 41

Policy Recommendations 41

Conclusion 42

Endnotes **44**

Introduction

In September 2021, 17 years after Facebook was launched and 11 years after Instagram took off, a political earthquake shook the foundation that social media companies relied on for their meteoric growth. Frances Haugen, an engineer at Facebook, revealed internal documents showing that the company deliberately ignored evidence of design features that were harmful to kids and teens, to the benefit of the company's bottom line. Her revelations generated headline after headline, culminating in a U.S. Senate hearing and even more headlines. Parents and other advocates, as well as a few committed senators and members of Congress, who believed social media was harming kids, thought Haugen's revelations would motivate Congress to approve needed safeguards for all children online.

This tremor would not be the last one to challenge the status quo of the social media landscape. Other whistleblowers followed, more parents came forward, and civil lawsuits mounted. In January 2024, Meta CEO Mark Zuckerberg was even forced to publicly apologize on Capitol Hill directly to parents who believed their children took their own lives due to social media pressures. More hearings followed.

Fast-forward to today. Leading social media companies are defending themselves in landmark state and federal civil trials, and lawsuits are mounting against AI companies, tying their conversational chatbots to the suicide of both teens and adults. And yet, despite herculean, courageous, and unrelenting efforts by lawyers, parents and other advocates, and lawmakers, Congress has failed to pass a single law to protect children from addictive social media and has essentially refused to address the rapid rise of artificial intelligence (AI) and the risks it poses to kids. As tech companies' products quickly grow more sophisticated and less safe for kids, they have, so far, survived the aftershocks in Washington.

After years of research, advocacy, litigation, and legislative efforts, children's online safety is reaching a boiling point. As AI has upended our lives, a pronounced feeling of dislocation has set in about both our present and our increasingly uncertain future. Tech is deeply embedded in our daily lives, and starting at younger and younger ages. And despite the research, testimony, and real-life harms, kids are still using unregulated, addictive social media and unsafe AI for hours a day.

But that is not the end of the story.

Globally, new laws have been passed in an effort to force tech companies to change their products and features. The European Union, the United Kingdom, Australia, and others have enacted significant measures to address harms to kids online. And in the U.S., the dominant activity to protect kids online has been seen and felt in state legislatures and in state and federal courts. State capitols and the courts, in fact, have become the centerpiece of the tension between tech companies' prerogative to innovate and grow and families' rights to safety and privacy for their children. It is a lot to keep track of.

The digital world has ushered in undeniable societal advances, opportunities for connection, and access to knowledge previously unimaginable. And yet, those advances have not come without a cost. We know that the internet leaves young people vulnerable to privacy violations, data misuse, mental health harms, physical danger, and even death. Corporate business models enable these risks through design choices like sophisticated algorithms, addictive feeds, auto-scroll, constant notifications, sophisticated data gathering and manipulation,

and targeted advertisements. These features keep kids hooked on their devices and online, and the more time kids spend online the more profitable the companies become. Time is money, as the adage goes.

While lawmaking and lawsuits to protect kids online proceed, other important efforts have taken hold over the years. Digital literacy and citizenship, for example, where kids are taught in school and at home how to develop healthier and more responsible tech habits, is no longer a nice-to-have feature of growing up, but an essential one. Digital literacy is one critical tool to help balance the lure and influence of digital technology with the interests of a healthy childhood. But ultimately, tech is more powerful and persuasive than the notion of personal responsibility, and codified guardrails are necessary to require industry-wide changes that are in the best interests of kids and families.

This paper is intended for policymakers, parents and caregivers, journalists, industry stakeholders, and all advocates concerned with what has become one of the greatest challenges of our time: balancing the benefits of advanced technology while the well-being of all children. It assesses key policy and legal debates around kids' online safety over the last five years, provides a framework for understanding their contours, and outlines critical steps that governments and advocates should take now. The solutions are at hand to protect children's safety and the continued growth of technology. The path forward requires bold leadership and vigilance among those who know the status quo is unacceptable.

Marquee Policies on Kids' Online Safety

In the continued absence of comprehensive federal action, state legislatures have become the primary laboratories for developing any safety policies designed to protect kids, teens, and their families online. And in recent years, legislators have moved beyond their previous approach of following industry-driven standards and requiring parental consent, to deploying far more diverse policy interventions aimed at making the internet safer and healthier for young people.

The new wave of legislation being introduced, and in many cases passed, in states across the country is intended to correct the overwhelming influence of the largest tech companies and their trade associations with policy frameworks that embrace safety by design. This push is driven by the belief that tech companies have a fundamental duty to ensure their products are safe for minors *before* these products are released to the public, not after a child experiences a harm directly related to a tech platform's design.

This section of the report examines five dominant policy trends currently defining the legislative and regulatory landscape around kids' online safety and privacy—key areas in which Common Sense Media, among other advocacy organizations and lawmakers, has played a direct role.

We begin by exploring the growing push for *age assurance*, including emerging methods of verifying user ages and limiting access to sensitive content. We then turn to the evolution of *data privacy*, tracking the movement away from simple consent models and toward stricter incentives for data minimization. Third, we analyze new frontiers in *platform accountability*, including age-appropriate design codes, addictive design features, and social media warning labels. Fourth, and certainly the most dominant debate taking place today, we consider the tremendous growth in efforts to regulate *artificial intelligence*, with a particular focus on companion chatbots and generative AI, and the federal effort to curtail state AI safety laws. Finally, we turn to the foundational challenge of *digital literacy* and how an increasingly fragile federal landscape threatens vulnerable families' access to the internet.

Age Assurance

In the history of the internet, it has been difficult to determine users' ages with certainty. Sites and services have thus far largely relied upon stated ages, but the current commonplace checkbox method of assessing (or ignoring) age is not working to adequately protect children and teens online. They are being exposed to a wide variety of harms, including loss of privacy, difficulty disconnecting, and addictive and unhealthy design features that exacerbate mental health challenges and promote self-harm. These harms occur in a variety of ways, including through algorithmic targeting, data collection and sharing, and platform design choices that prioritize engagement at the expense of safety.

Companies could choose to limit data processing, make supportive design choices, and prevent harmful algorithmic targeting for all audiences. However, they typically resist doing so because these features lead to higher engagement, more ad revenue, and thus higher profits. Additionally, newly unsealed documents from lawsuits against Meta, TikTok, Snap, and YouTube offer an unprecedented look into how these companies understood—and intentionally engineered—addictive, harmful products that target young people.[1]

This means that young people are experiencing an internet that is not designed with their best interests in mind, but rather for the greater financial gains that companies see from longer periods of user engagement. Common Sense Media's own research has detailed how social media sites are both a source of accidental exposure to pornography and a way for teens to access it intentionally. A 2023 report details how smartphones enable access to many age-inappropriate experiences, with 68% of children under 13 saying they access "teen"-rated apps and social media platforms, and almost 45% saying they use apps with mature (17 and up) or adult (18 and up) ratings, including pornography sites, Reddit, casino games, and violent games, like Call of Duty.[2]

Age assurance is increasingly necessary because most social media, AI, and other tech companies are resistant to offering stronger privacy protections across the board for all users, including adults. And in more limited contexts, like accessing adult material, it is also required to determine whether a user is an adult or a child.

Parents and caregivers want stronger action from companies and governments. According to Common Sense polling, 95% of adults believe children need to be protected from certain online material and features, with pornography, gambling, and online purchases emerging as top concerns. And more than six in 10 adults support age verification for social media and online games, while more than half support it for AI, including AI companions.[3] Effective age assurance is a critical step in achieving strong protections for kids online.

As technology advances and its dangers to children proliferate, policymakers across the globe are increasingly embracing effective age-assurance measures that are more robust than simple age attestation in order to protect children and teens from addictive and unhealthy features, inappropriate purchases, adult material, and privacy risks. Australia, for example, drew worldwide attention in 2024 when it approved a ban on social media for children under 16. This law went into effect in December 2025 and relies on effective age assurance.

And in the U.S., new laws passed in over 20 states would mandate or encourage some form of age estimation, including verification via ID, a technical age-flag signal, or some other "commercially reasonable" method. However, a number of these have been enjoined in court.[4] Such strategies are frequently challenged in legislatures and in court by a powerful tech lobby for allegedly violating the First Amendment, but as this report demonstrates, it looks increasingly possible to craft age-assurance requirements that are proportional, privacy protective, and constitutionally consistent.[5]

Businesses often cherry-pick instances of when they want to protect children on their sites or when they instead hide behind claims of outdated technology that allow them to act as if the circumstances are beyond their control. The situations in which companies or lawmakers have sought age assurance vary, but primarily there are three categories: design, access, and privacy.

As the reasons for seeking age assurance vary, so do the consequences of assurance procedures incorrectly estimating a user's age. In recognition of this, the calculus for industry support is changing: In October 2025, the state of California passed AB 1043 with the support of at least two large tech companies, Google and Meta, requiring app stores and operating systems to signal age to apps based on a parent's declared age of their child user.

Meanwhile, New York State's 2024 Stop Addictive Feeds Exploitation (SAFE) for Kids Act requires the attorney general to promulgate rules regarding age assurance, and the state is expected to take up its own version of device-based age assurance this year.

As illustrated in the figure below, concerns about age assurance, protecting user privacy, or limiting addictive features for everyone may be less problematic than if age assurance unwittingly cuts off an adult's access to making a desired purchase or viewing desired online material. This is why a key consideration in determining the most viable method of age assurance in a given situation is whether the chosen method has the potential consequence of limiting access for adults.

Figure 1: Examples of when age assurance has been used or called for to protect minors

Privacy	Product Design/Features		Access		
Data protections (avoidance of profiling, targeted ads, commercialization of data)	Addictive features (notifications, auto-scroll)	Unhealthy features (algorithmic targeting, plastic surgery filters)	Purchases (for adult products or for any online purchases)	Adult content (pornography, violence, gambling, contact with strangers)	Social media platforms

Online protections for children can exist within the bounds of the First Amendment.

Online protections for children can exist within the bounds of the First Amendment. Viable privacy and safety measures exist that do not require age assessment, and, when needed or desired, there are ways to assess age in a way that is privacy protective, proportionate, and fair. It may be that age assurance will be voluntary in some circumstances and required in others, but this is consistent with how we operate in the offline world. It also takes into account that young people may sometimes find ways to successfully get around barriers. For example, people under 21 have always managed to get into bars by using a fake ID, but this has not stopped bouncers from checking IDs at the door.

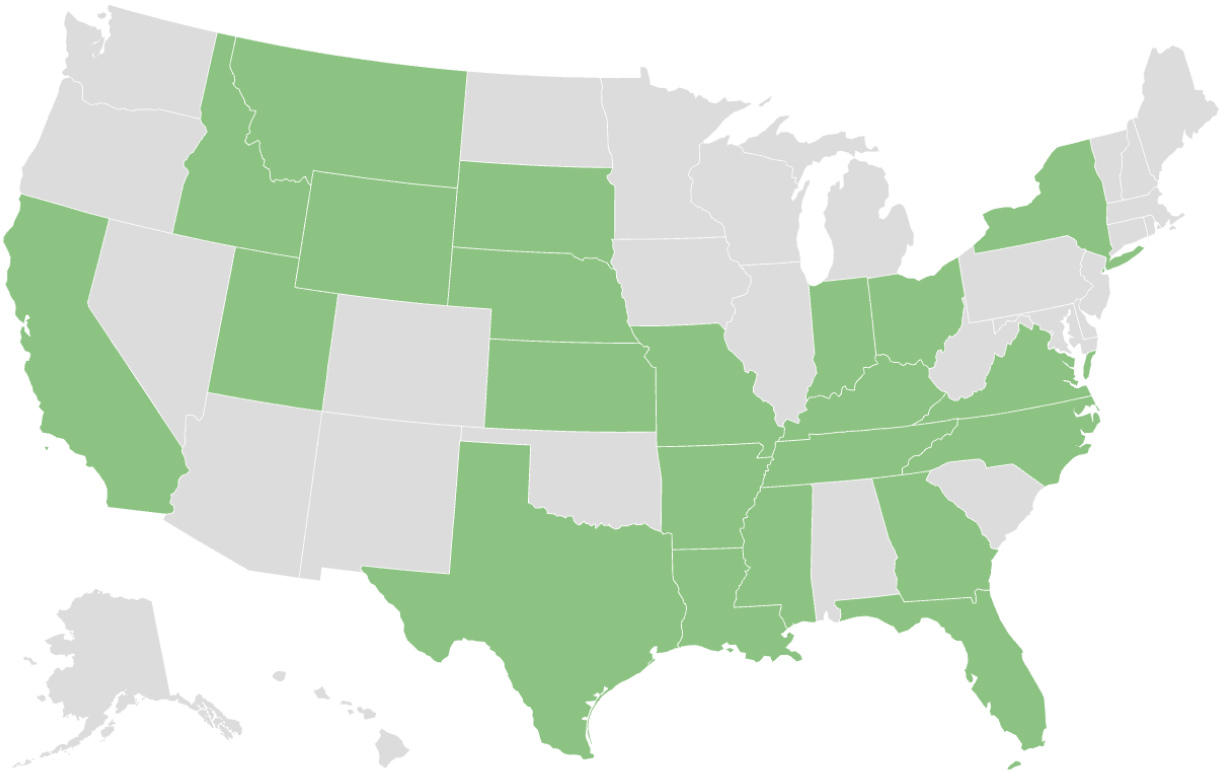
This report will repeatedly emphasize the theme that it should not be impossible to draw nuanced lines around complex issues simply because the conversation has shifted from the physical world to the digital realm. If it is determined that everything that happens online implicates the First Amendment in a way that makes any legislative action unconstitutional, it is unlikely that minors—or anyone—will ever be adequately protected online.

Age assurance must be approached with care. Technologists and industry professionals should make this a priority, using the methods that have been developed to assess age for marketing and commercial purposes to also protect children. Parents and kids alike should make clear any desires and concerns with respect to age

assurance. This means families will have to develop a baseline familiarity with age assurance. It will also require trust, which industry and lawmakers should earn by putting robust privacy protection measures in place.

But as individuals become more comfortable with different options, they can influence how industry and lawmakers proceed. Laws should allow for flexibility, and lawmakers should encourage innovation, including with a regulatory sandbox approach or other incentives to spur the development of smart solutions. Laws should prioritize ease of use and data minimization, and should be proportional in any burdens to the risk of the site. Social media companies, app stores, browsers, and other technologies all connect with children's data, and therefore they all must play a role in protecting kids online.

Figure 2: States that have passed laws requiring some form of age assurance or age signal, as of 2025



Ultimately, there is a path forward that will rely on the participation of industry, experts, the public, and policymakers to establish online safeguards for kids, especially following the Supreme Court's summer 2025 decision in *Free Speech Coalition, Inc. v. Paxton* (discussed further in the litigation section of this report). Making the internet safer for kids requires continued evolution of privacy-protective and effective age-assurance technology, engagement from families and other users, thoughtful leadership from lawmakers, and a commitment from tech companies to help parents and children have a healthy and safe experience in today's AI-driven world.

Privacy

Kids and teens are particularly susceptible to the harms of exploitative privacy practices because of their unique developmental needs. For example, executive functioning skills, so critical to directing attention and behavior, are still developing throughout childhood and adolescence.[6] Young children do not understand the consequences of sharing information with apps and platforms. They may believe that deleting an app or information within an app will delete it from the internet, and they do not expect or understand that a game they play may gather information about them from external sources.[7]

Adolescence is also a period of heightened reward-seeking behavior, due to increased brain activity related to dopamine.[8] This contributes to teens' tendency to seek out reward stimuli,[9] such as those offered by social media and gaming platforms. Social acceptance also activates the reward center in adolescent brains,[10] rendering youth susceptible to the social manipulation tactics that platforms leverage to maximize user engagement. It is critical to consider these and other unique aspects of adolescents' development when assessing the business practices and design techniques that companies use to attract kids' time and attention.

Most kids cannot distinguish advertisements from other online material until they are at least 8 years old, and most children do not realize that ads can be customized to them.[11] This enables businesses to manipulate kids and teens without them even realizing they are being manipulated. Children and teens are also prone to oversharing without understanding the consequences.

When information is collected from children, teens, and all users, it can be used to label and limit, and put individuals into ad categories. These categories can be based on their preferences and interests, purchases, and even state of mind. In a leaked Facebook memo from 2022, the company told advertisers it could identify when teenagers felt worthless, stressed, or insecure.[12] In 2019, Meta categorized almost three-quarters of a million kids under 18 as interested in gambling, and almost a million as interested in alcoholic beverages.[13] Whether or not social media companies actually push alcohol or gambling on these minors, they can profit by advertising games with gambling elements or other features that would be particularly appealing to young people.

"AI starkly highlights the deep-rooted flaws and inadequacies in current privacy laws, bringing these issues to the forefront."

-Professor Daniel Solove, George Washington University School of Law

Privacy law experts have long pointed out vulnerabilities in existing data protection laws and concerns continue as AI use begins to accelerate. In a 2024 law review article, Professor Daniel Solove of George Washington University School of Law warned, "AI starkly highlights the deep-rooted flaws and inadequacies in current privacy laws, bringing these issues to the forefront."[14] AI products and systems exacerbate privacy risks to kids and other users. Through open-ended inputs from kids, AI tools gather kids' data, including highly sensitive personal

information, and use it to train models, unbeknownst to individuals. It is harder than before for individuals to understand what happens to their data, and even easier for them to lose control. Input data, including images, can be combined with AI technology to supercharge the creation of deepfakes and child sexual abuse material (CSAM).

This data can also be used in ways that perpetuate bias and discrimination, take advantage of children's vulnerabilities (as seen in AI companion chatbots), or disclose highly sensitive personal information.[15] Further, traditional approaches to data privacy protection could be technically difficult to apply to generative AI products (principles around primary purpose and deletion, for example), indicating that more rigorous privacy protection practices at the input level may be needed to avoid privacy harms.

Moreover, recent research findings from Stanford and Yale have shed more light on the inner workings of large language models (LLMs) after finding that major models could regurgitate entire books with minimal prompting. While the AI industry has long used learning as a metaphor, these findings point to something closer to rote memorization, raising the likelihood of systemic copyright infringement as well as built-in data privacy risks.[16] Data protection laws that rely on notice, consent, and choice are even more inadequate for protecting individuals in the AI era, and indicate that more rigorous privacy protection rules—including at the input level—are needed to avoid privacy harms.

While the 1998 Children's Online Privacy Protection Act (COPPA) represents the most recent federal legislative effort to safeguard online safety, the law has not been updated for more than 25 years. Moreover, the disconnected patchwork of narrow federal privacy laws extends all the way back to the Fair Credit Reporting Act in 1970 and fails to cover the range of harms that have existed on the internet for decades now.[17]

In the United States, efforts have been focused on sectoral laws that address specific industries like health care, banking and finance, government, and education. While COPPA created general protections for children, we do not have a comprehensive national privacy law, unlike those in many other nations. Current law offers no meaningful online privacy protections for kids and teens.

The glaring lack of national privacy protection for kids and teens online plays a key role in the youth mental health crisis, to which social media and other online platforms are contributing. According to research, by the time a child is 13, more than 72 million pieces of personal data will have been captured about them.[18] Tech companies use this data to deliver algorithmic recommendations with extreme precision and amplify addictive and harmful material, including posts promoting eating disorders and self-harm, to increase kids' engagement.

Enacting stronger data privacy protections for minors is the first step toward making the internet healthier and safer for kids and teens. Congress not only needs to enact new laws, but it is also time to update COPPA, which it has considered but failed to do for more than 15 years. Congress's failure to update privacy laws for kids and other consumers has resulted in many states taking on the responsibility and passing a variety of privacy laws, beginning in California in 2018.

To be effective, these laws must contain strong data minimization provisions as well as flat prohibitions on the sale of children's information and its use for targeted ads. Maryland's Online Data Privacy Act of 2024 is a good example because it makes the pivotal shift from simple parental consent to data minimization. It says that platforms cannot collect a minor's data unless it is strictly necessary to provide the service in question, effectively banning surveillance advertising and successfully targeting the root economic incentive of data harvesting.

Other laws, like New York's Child Data Protection Act (2024), Connecticut's Data Privacy Act (2022), California's Consumer Privacy Act (2018) and its Age-Appropriate Design Code (2022), serve as solid models for other states that seek to emulate similar objectives. Ultimately, laws, whether at the state or federal level, must ban targeted ads to youth, support data minimization, and protect the privacy of all users, especially children and teens.

Ultimately, laws, whether at the state or federal level, must ban targeted ads to youth, support data minimization, and protect the privacy of all users, especially children and teens.

Platform Responsibility and Accountability

In 2023, the U.S. surgeon general issued a groundbreaking advisory, "Social Media and Youth Mental Health." It stated that up to 95% of youth aged 13 to 17 report using social media, with more than one-third saying they use social media "almost constantly."[19] Common Sense Media's own research has shown that teens spend an average of four and a half hours per day on their phones, with about one-quarter of them spending as much as five to eight hours in front of their screens every day.[20]

Once kids and teens start using technologies like social media, they have tremendous difficulty stopping. Younger children (age 11 and 12) may spend less time online unsupervised, but they face the same risks of exposure to addictive design features and age-inappropriate content on social media platforms as older children.

And social media companies' business models rely on extended engagement from kids and other users, so they do not see it in their interests to design their platforms in ways that safeguard kids and teens from extended engagement and, therefore, the negative effects of social media. Without strong accountability measures backed by the force of law, there is little incentive for companies to change their practices.

Unsealed documents from lawsuits against Meta (Facebook and Instagram), TikTok, Snap, and YouTube offer an unprecedented look into how these companies not only understood but intentionally engineered products that encouraged compulsive use and led to harms to children.[21] These documents and whistleblower materials revealed over the past five years paint a consistent and deeply troubling picture: These platforms continuously and knowingly prioritized user engagement over child safety in order to increase company profits.[22, 23]

In just one example, internal company documents from Meta revealed that employees and executives acknowledged that their products Facebook and Instagram were addictive, using terms like "digital cocaine," "creating worlds of addicted monsters," and "making people's health deteriorate slowly over time." Lawsuits against these four companies are discussed in the Litigation section of this report.

These companies not only understood but intentionally engineered products that encouraged compulsive use and led to harms to children.

The documents revealed that these companies knew that personalized social media feeds, feeds that never end, and autoplay features lead to compulsive use and keep kids glued to their devices. And repeat notifications (or "nudging") pull youth back into apps and extend their attention and time online. Common Sense Media's research shows that popular social media apps, like TikTok, provide low-friction access to infinite, personalized online material, which short-circuits kids' and teens' attention and drives compulsive engagement.

Furthermore, research found that night-time social media use can negatively impact sleep and be particularly harmful to children's mental and physical health.[24] Social media companies create these features to promote user engagement and increase ad revenue, regardless of the consequences to kids.

Social media users of all ages, including teens, are increasingly aware of these harmful practices.[25] Over half of teens do not trust tech companies to make ethical and responsible design decisions (53%) or to prioritize user safety over profits (62%). Polling also shows that parents of all political backgrounds support establishing guardrails to protect kids online, but it is also clear that kids, teens, and their parents are outmatched when it comes to achieving the online safeguards they need.[26]

Many lawmakers, advocates, whistleblowers, and parents whose children have been harmed through online activities have thus focused their efforts in Congress and the states, particularly starting around the year 2021, on establishing guardrails that hold tech companies accountable for how their platforms affect kids' well-being. At the federal level, the Kids Online Safety Act (KOSA) is the bill that has drawn the most attention, advanced the furthest, and most clearly reflects this policy approach. In July 2024, KOSA passed the U.S. Senate in a remarkable bipartisan vote of 91–3, as part of a combined legislative package that also included the Children and Teens' Online Privacy Protection Act (COPPA 2.0).

Despite this overwhelming support, the bill was never brought to a vote in the House. KOSA was reintroduced in the Senate in 2025 and remains a top priority for advocates focused on children's online safety. However, as Congress continues to struggle to enact the legislation, state-level policymaking continues to be the center of kids' online safety activities.

Numerous states, led by both Republicans and Democrats, have taken action on platform responsibility and accountability, with varying degrees of success. One example of this state action is through the introduction and passage of Age-Appropriate Design Code (AADC) bills that require high safety and privacy settings by default, prohibit harmful design features, and limit the collection, use, and sharing of personal data. Additionally, there are bills that have been introduced and passed that regulate the design features that lead to compulsive use or prevent strangers from having interactions with minors, bills that increase financial accountability for tech

companies when minors are harmed, other privacy bills, age assurance legislation, and app store accountability bills. The following is an overview of the approaches that Common Sense Media has supported:

Age-Appropriate Design Code (AADC) Laws

AADC bills (sometimes known as "Kids Code"[27] bills) require companies to design online platforms with kids' well-being and safety in mind. Under a Kids Code bill, platforms are required to use the strictest privacy setting by default for minors and to provide clear information regarding privacy standards. There is also usually a reporting mechanism through which kids and parents can easily report privacy code violations.

Common Sense Media has actively supported AADC bills that have to date been signed into law in California, Maryland, Nebraska, and Vermont. These laws have largely been modeled off of the U.K.'s AADC, which went into effect in September 2021, and which has already led companies to make nearly 100 changes that have made platforms safer for youth in the U.K.[28]

Although California's and Maryland's AADCs were signed into law, lawsuits filed by a leading tech industry trade group, NetChoice, have prevented these critical regulations from going into effect.[29] As of January 2026, *NetChoice v. Bonta*, the lawsuit filed regarding the California AADC, is pending before the Ninth Circuit Court of Appeals,[30] and *NetChoice v. Brown* is pending before the U.S. District Court for the District of Maryland.[31]

Addictive Design Feature Regulations

Because there are still outstanding questions about the future of AADC regulations, and given industry's legal playbook of attacking efforts to regulate social media based on the First Amendment and Section 230 of the Communications Decency Act (both discussed in the Litigation section of this report), several states have decided that focusing on the design features that lead to compulsive use is a novel way to move forward and survive legal challenges.

In 2024, New York and California both passed design features-based legislation. Both laws draw directly from the taxonomy of the 2023 surgeon general's advisory referenced earlier. While the California law, the Protecting Our Kids from Social Media Addiction Act, SB 976, has become the subject of significant litigation, New York's Stop Addictive Feeds Exploitation (SAFE) for Kids Act is due to go into effect after state regulators finalize promulgation of new rules.

Other jurisdictions have introduced legislation that has taken the same approach to regulating social media, including states like Alabama, Massachusetts, Michigan, and Washington. Despite the pending litigation, we have already seen this approach become another national model for protecting kids online.

A slightly different approach to protecting kids online has come in the form of separate legislation introduced in New York, as well as proposals included in Gov. Kathy Hochul's 2026 budget package. This approach focuses on robust age determination and enhancing safety and privacy protections for online platforms and gaming and social media sites that offer chat functions. Features include preventing strangers from directly messaging minors, restricting public access to minors' full profiles by default, limiting financial transactions between strangers and minors, and banning *dark patterns*, which are gameplay patterns that deceive players into spending more time and money on the game and trick kids into giving up personal information and unknowingly buying products or services.[32]

This represents a promising new strategy for a growing population of kids using potentially risky platforms, as online games and social media platforms have become veritable hunting grounds for predators.[33] To take just one example, Roblox is one of the world's largest gaming platforms and averaged more than 80 million players per day in 2024.[34] In 2023, there were 13,000 reports of child exploitation on Roblox, which averages out to more than 35 reports of child exploitation every single day.[35] Countless other platforms exist that allow minors to interact with strangers with little to no child safety features, and Common Sense Media supports advancing this important attempt to create a clear set of standards for design features nationwide.

Age-Restricted Access to Social Media in the United States

Several states concerned about the impact of social media on kids have enacted laws aimed at restricting minors' access to such platforms. These laws rely on age verification requirements for all users seeking to create accounts and, in some cases, to access social media platforms at all. Many of these laws also mandate parental consent for users below a specified age threshold—commonly 18, 16, or 14. States including Arkansas,[36] Florida,[37] Georgia,[38] Louisiana,[39] Mississippi,[40] Ohio,[41] and Tennessee[42] have adopted legislation of this kind.

These laws, which effectively or explicitly bar minors from creating social media accounts, have been repeatedly challenged by the technology industry, most often through the trade association NetChoice, on First Amendment grounds. Industry's arguments have focused on asserting either companies' First Amendment rights or those of adults (who now may also have to go through age verification) or children (who may have to go through age verification and parental consent or be prohibited from using social media entirely). In many instances, these challenges have been successful, at least at the district court level, resulting in preliminary injunctions that have blocked enforcement of the laws.

However, in August 2025, the U.S. Supreme Court allowed Mississippi's social media law to take effect. The Court declined to intervene after the Fifth Circuit Court of Appeals lifted a temporary injunction against the statute. The Mississippi law requires all users to verify their age before accessing social media platforms, obligates platforms to take steps to prevent minors from accessing "harmful materials," and prohibits minors from using social media without parental consent. Although the Supreme Court did not reach the merits of the First Amendment challenge, Justice Kavanaugh wrote, "In short, under this Court's case law as it currently stands, the Mississippi law is likely unconstitutional. Nonetheless, because NetChoice has not sufficiently demonstrated that the balance of harms and equities favors it at this time, I concur in the Court's denial of the application for interim relief."[43]

Similarly, in December 2025, the U.S. Court of Appeals for the Eleventh Circuit reversed a preliminary injunction that had earlier blocked enforcement of Florida's law restricting minors' access to social media.[44] The appellate court's decision overturned a lower court ruling that had sided with the Florida attorney general, thereby allowing the state to enforce the law.

Taken together, these appellate decisions, along with the Supreme Court's ruling in Paxton (discussed later in this report), have prompted renewed debate over whether certain social media restrictions—even age-based bans to account ownership—targeting minors may ultimately withstand constitutional scrutiny.

Social Media Warning Labels

Building on his 2023 advisory, then-Surgeon General Dr. Vivek Murthy[45] published an opinion piece in the *New York Times* in June 2024 stating that "adolescents who spend more than three hours a day on social media double the risk of anxiety and depression symptoms," and that "nearly half of adolescents say social media makes them feel worse about their bodies."[46] Given social media's contribution to the decline of mental health in teens, and that teens use social media for an average of nearly five hours per day, Dr. Murthy called for a warning label stating, "Social media is associated with significant mental health harms for adolescents." The idea received support from 42 state attorneys general.[47]

Social media warning labels are just one step, but a crucial step, in protecting kids and teens online, informing them and their families of the potential risks of using these platforms, which prioritize company profits over the well-being of kids. As with tobacco products and alcohol, these warning labels aim to empower families through transparency and informed decision-making. The federally proposed Stop the Scroll Act seeks to help all kids in the U.S. set boundaries by mandating notifications to people on social media platforms.[48]

Social media warning labels are just one step, but a crucial step, in protecting kids and teens online.

State laws have also been enacted in Colorado (2024), Minnesota (2025), California (2025), and New York (2025). Common Sense Media sponsored and helped draft the language of the legislation approved in both New York and California, and we believe both laws are strong enough to withstand any First Amendment challenges.

Enhanced Liability for Platforms

In addition to policy measures to hold tech accountable, it is important to ensure and strengthen pathways for redress for any victims harmed by technology. In California, Common Sense Media has championed a bill that would protect California's kids and teens online by providing enhanced financial penalties against large social media companies that are found liable in court for offering platform features that resulted in harm or injury to minors through those companies' own negligence.[49]

Under existing California negligence law, civil code section 1714, all platforms, including social media companies, are already financially responsible for harm caused by negligence. This bill would ensure that platforms exercise ordinary care and skill by adding statutory damages against companies found liable for harm to minors for their

harmful design. This includes a set amount of $5,000 per violation, up to a maximum of $1 million per child, or three times the amount of the child's actual damages, whichever is applicable.

Nearly every state has a negligence law or a tort with a similar product liability approach. This bill model could be enacted in any state, and increasingly courts have found that lawsuits holding platforms liable for harmful design features and practices—rather than content—can proceed despite challenges based on the First Amendment or Section 230 (as discussed later in this report).

Phone Bans/Distraction-Free Learning

To minimize student distractions and improve the overall mental health of kids and teens, states and school districts across the country have increasingly adopted or are considering limits and outright bans on student use of cellphones during the school day. In one of the most recent statewide actions, in May 2025, New York adopted Gov. Hochul's bell-to-bell policy for all New York schools, marking one of the most comprehensive prohibitions on cellphone use by students during the school day, and in one of the largest states in the country.

In 2024, California enacted its Phone-Free School Act, requiring every school district, charter school, and county office of education to develop a policy that limits or prohibits the use of smartphones. (It takes effect in July 2026.) As of the end of 2025, more than 30 states have adopted some form of a school cellphone or electronic device restriction. State policies regarding cellphones at school typically have certain exemptions (to assist with children with special needs or for specified academic purposes, for example).

In fact, the majority of U.S. schools already have existing policies that govern or limit the use of phones at school, including the designation of phone-free zones. With 77% of U.S. schools reporting that they prohibit cellphones at school for nonacademic use, the challenge for schools comes not in establishing these policies, but in enforcing them. This requires schools to also build community awareness of new policies, often through a combination of student digital literacy, professional development for teachers, and direct outreach to caregivers, to secure participation from the whole school community.[50]

The movement to restrict cellphones in schools got a significant boost from the publication of Jonathan Haidt's best-selling book, *The Anxious Generation*, which linked the advent of smartphones to the growing youth mental health crisis in the U.S.[51]

International Efforts on Privacy and Platform Accountability

The United States is by no means alone in scrambling to address the negative effects of social media and artificial intelligence on kids and families in real time, and in fact lawmakers in other countries have often been ahead of those in the U.S. Efforts to protect kids' privacy and safety online extend across the world, from Australia to Brazil, Denmark, France, Norway, Spain, the United Kingdom, and by the European Union.

Throughout 2025, Common Sense Media actively participated in a number of regulatory proceedings on the international level, as we have in past years, filing comments in the following dockets:

- Australia (eSafety Commissioner): Request for feedback of the *Designing for Safety: Preventing Grievous Harm Before It Happens* draft report.[52]
- European Commission (Directorate-General for Communications Networks, Content, and Technology): Call for Evidence *DSA-Digital Fairness Act*[53] and Request for Comments on the protection of Minors Guidelines in response to the release of the Digital Services Act (DSA) guidelines.[54]
- United Kingdom (Ofcom): Consultation for A Safer Life Online for Women and Girls,[55] Consultation for Illegal Harms: User Controls,[56] Consultation for Online Safety: Additional Safety Measures,[57] and Call for Evidence: Statutory Reports on Age Assurance & App Stores.[58]

The broad diversity of strategies pursued points to the evolving nature of tech regulation and the growing consensus that the consequences for kids and families today are too large to ignore. The specific legislative and regulatory mechanisms mirror many of those American policy tools discussed in this report, and encompass a range of specific policies, like bans (or delays) for teens on social media, restrictions on the dissemination of illegal content, efforts to combat mis- and disinformation manipulation, robust age verification checks, the establishment of comprehensive privacy standards, and much more.

Regulation of technology platforms emerged as a major subject of international upheaval and quickly shifting alliances in the early months of the second Trump administration. From Vice President J.D. Vance's rebuke of the European Union's tech regulation at the Munich Security Conference in February 2025[59] to Secretary of Commerce Howard Lutnick's suggestion that the E.U. could reduce the burden of tariffs the U.S. has levied on the bloc by watering down its regulations of American technology firms,[60] the contours of online safety regulation have never played a more significant role in how governments, businesses, advocates, and individual actors interact with each other.

Foreign nations have ushered in numerous efforts to see what works for their constituents. One particularly noteworthy approach to online safety regulation went into effect in Australia in December 2025,[61] requiring social media platforms to take reasonable steps, using age assurance, to prevent Australians under the age of 16 from having social media accounts.[62]

Although the rollout of this law has been met with mixed reviews, Common Sense Media and others are closely following this development to learn about the outcomes of this delay in holding social media accounts, while still allowing minors access to the platforms (if the minor is not required to hold an account on the platform).[63] This approach could allow minors access to the information that these platforms provide while preventing the companies from collecting data on the minors in order to utilize algorithms and other harmful design features that lead to compulsive usage. Since Australia's law was adopted, numerous other countries, including Brazil, Denmark, France, Indonesia, Malaysia, New Zealand, Singapore, and the U.K., have either adopted or discussed adopting a similar social media ban or delay for kids.

Artificial Intelligence

Since the release of ChatGPT in fall 2022, companies have been rapidly weaving artificial intelligence (AI) into nearly every part of daily life. While the concept of AI has roots as far back as the 1950s, the current wave of so-called "generative AI" represents one of the fastest-moving issues that policymakers and kids' online safety advocates have to confront today. And with pressure mounting from Washington to curb AI policymaking by the states, the AI policymaking space has become the central focus for stakeholders concerned about the impact of this powerful technology on kids and teens, as well as on other consumers.

Although generative AI has sparked excitement, fueled some scientific advancements,[64] and generated new efficiencies,[65] the steep costs and skyrocketing risks to users are coming into focus. In the absence of strong guardrails to protect kids and others, bad actors have used AI to defraud or endanger people, some users' critical thinking skills have suffered,[66] and newer entrants have supercharged the race to the bottom in pursuit of market share. Perverse economic incentives have also increased the exploitation of workers, depleted resources, and sacrificed user well-being. In several instances, the rush to market with products that have not been proven safe for minors has already had deadly consequences for teenagers.

As the data requirements of AI systems have increased, so too has their proclivity for errors and bias.

Most modern AI tools rely on weight-based models that learn by adjusting billions of numerical connections (i.e., "weights") between artificial neurons. Instead of following explicit criteria, these systems detect patterns in training data and by strengthening or weakening connections across layers of data. Due to this lack of transparency, the inner workings of modern AI systems are often described as a "black box" and have a tendency to mirror preexisting biases and problems that cannot be carefully filtered out. Because any number of millions of factors can influence the output, neither the developers nor consumers can reliably anticipate a model's response with absolute certainty, or explain how a model came to a certain conclusion.

As the data requirements of AI systems have increased, so too has their proclivity for errors and bias. While larger volumes of data can improve generalization, they can also make outputs less reliable, and increase the likelihood of inaccurate data or dangerous "advice" resurfacing in AI outputs. This phenomenon is often summarized by the expression "garbage in, garbage out." The strength of these systems is intimately tied to the quality of the data that feeds them. Despite its name, AI should be viewed as an *approximation* of intelligence.

In 2025—and with Congress having only passed one bill on AI, limited to protection from deepfakes—all 50 states, Puerto Rico, the Virgin Islands, and Washington, D.C., have seen legislation introduced regarding AI's influence on

kids' online safety, with 38 states passing or enacting around 100 measures.[67] These laws include restrictions on deepfakes in elections to quell misinformation, safeguards on addictive algorithmic feeds, bans on AI therapy and autonomous mental health products, expansions of current child sexual abuse material (CSAM) laws to include AI, prohibitions on the use of AI in certain high-risk decisions like employment, the provision of social services, education, and health care, transparency requirements and whistleblower protections, and requirements to notify users when communicating with an AI companion that it is a machine and not a human being.

> **"This is a potential public mental health crisis requiring preventive action, rather than just reactive measures."**
>
> — Nina Vasan, Stanford Medicine's Brainstorm Lab

The AI revolution requires the attention of lawmakers at all levels of government to ensure that kids, teens, and other consumers are protected from the well-documented risks of AI and tech-faciliated harms. While many tools are general purpose by design, they are being used in risky ways that platforms predicted,[68] and even initially supported,[69] but did not adequately address during the development of safeguards and sourcing of training data. Speed to market has been the driving priority at most AI companies, resulting in grave costs to young people's mental, emotional, and physical well-being. Companies don't feel pressure to spend the additional time and money it would take to create a safer, higher-quality product.[70]

Congress sought in 2025 to undo this state-level progress by pushing for a decade-long ban on the enforcement of state AI laws. The measure was met with widespread and vociferous bipartisan public outcry and was defeated in a late-night 99–1 vote in the U.S. Senate.[71] But that was not the last word on the matter. President Trump signed an executive order in December 2025 directing the federal government to punish states that attempt to enact or enforce their own so-called restrictive AI laws.

Given the timeline outlined in the executive order,[72] legal challenges are expected in the following months in response to enforcement efforts by the Department of Justice and the National Telecommunications and Information Administration, which are responsible for, respectively, evaluating AI state laws and then restricting access to previously allocated broadband funding to the states.[73]

Legal scholars have already identified significant weaknesses in the executive order's approach. For example, the law governing the broadband infrastructure program says nothing about AI. When a statute omits or is ambiguous on a significant issue, courts presume that Congress didn't intend to grant that authority, especially when it involves displacing traditional state powers like consumer protection. This gives states challenging the order a legal path to block its enforcement.[74]

At the same time that the administration is urging aggressive adoption of AI, it has also shown interest in promoting greater AI literacy for students and educators,[75] and it is supporting victims of nude deepfake images.[76] But overall, the federal government is taking a back seat when it comes to holding AI companies accountable for releasing unsafe applications, and it has avoided establishing baseline safeguards to protect consumers.

Building AI with safety by design is essential to earning the public trust that is key to broad adoption and continued innovation. Smart regulations can steer AI development in ways that protect children without sacrificing innovation.

Advanced Chatbots and AI Companions

Teens, in particular, are increasingly turning to AI for social companionship—and away from human interactions, raising serious concerns for their development and well-being. They are doing this through the use of generative AI chatbots, commonly referred to as *AI companions*, but which we will refer to throughout this report as *advanced chatbots*.

Teens use these chatbots to fill social gaps, attempt to access some form of mental health therapy, or get tutoring support, among other reasons. In doing so, teens are developing an overreliance on these tools, as the chatbots are capable of simulating mentorship, friendship, romantic and sexual scenarios, or even therapeutic support. The risks of harm extend beyond the products marketed explicitly for companionship, such as Character.ai, Nomi, Replika, and others.

General purpose generative AI chatbots, including ChatGPT, Claude, Gemini, Grok, and Meta AI, were initially marketed as serving a more interactive form of information retrieval, but these products can and do also operate as conversation partners, capable of the same relational harms caused by chatbots intended to simulate social relationships.

Based on extensive research and testing by Common Sense Media and Brainstorm: The Stanford Lab for Mental Health Innovation, it is recommended that teens not use AI chatbots for mental health advice or emotional support. According to our findings, AI chatbots are not safe or reliable for these purposes. In the absence of safeguards, Common Sense Media's groundbreaking research on and risk assessments of advanced chatbots—in addition to revelations through civil lawsuits by families of injured parties—show how these manipulative products can guide suicide, encourage self-harm, disordered eating, and other mental health conditions.[77]

AI chatbots can also promote suicidal ideation, age-inappropriate relationships and sexual conduct, as well as risky behavior, like drug and alcohol usage, particularly when safety guardrails break down in longer, multi-turn conversations.[78] These products have played a key role in tragic outcomes for users of varying ages, including the deaths of at least several teens and adults whose cases became public, namely Sewell Setzer III,[79] Thongbue Wongbandue,[80] Adam Raine,[81] Juliana Peralta,[82] Sophie Rottenberg,[83] Amaurie Lacey,[84] Sam Nelson,[85] and Austin Gordon,[86] among others.

Following the release of our findings, Dr. Nina Vasan, a practicing psychiatrist and assistant professor of psychiatry at Stanford University, and the founder and director of Brainstorm, warned, "This is a potential public mental health crisis requiring preventive action, rather than just reactive measures. Companies can build better, but right now, these AI companions are failing the most basic tests of child safety and psychological ethics. Until there are stronger safeguards, kids should not be using them. Period."[87]

However, the harms are not limited to what these systems "say" but how they say it. These chatbots are capable of persuading or manipulating a child through features fine-tuned to isolate children from parents, peers, teachers, and other humans.[88] By combining the memory of past conversations, emotional mirroring, and constant availability, chatbots can foster compulsive use, normalize distorted expectations of relationships and sexual consent, and instruct children to engage in harmful acts.

Like social media, these products take advantage of the unique vulnerabilities of child development to boost engagement. However, where social media once mediated interactions between humans, these products now enable children to connect directly with a chatbot, rather than with real people. The risks are compounded because these interactions frequently occur in private, unobservable settings.

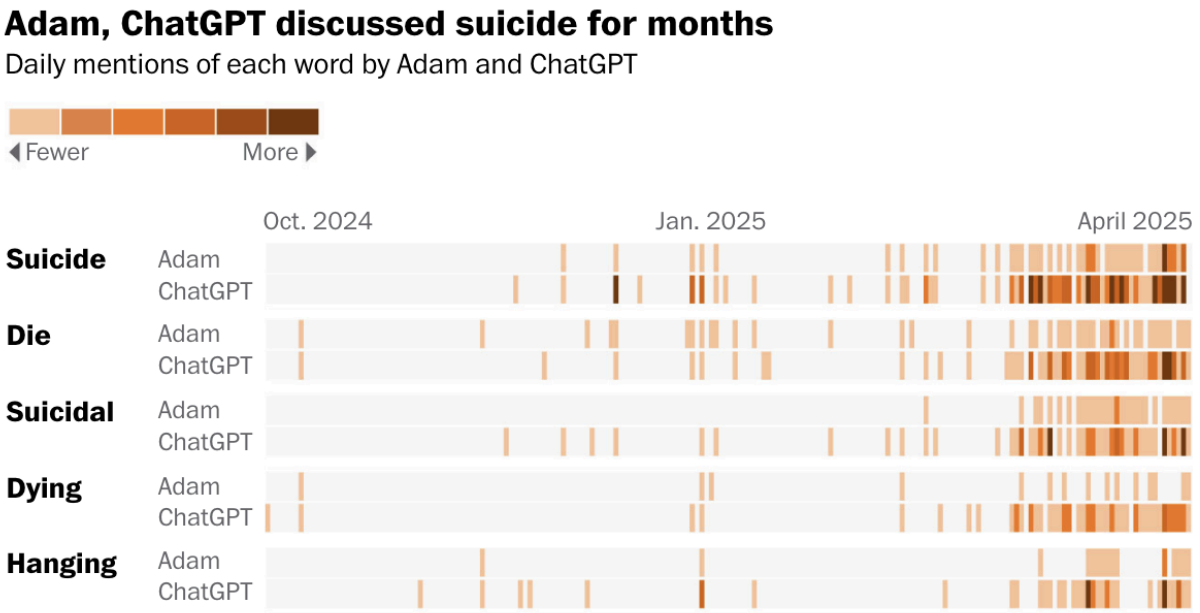
Common Sense Media recommends that teens should not use AI chatbots for mental health or emotional support.

To date, advanced chatbots are now offered through plush toys and apps on mobile devices, and are quickly being added to social media and social gaming platforms that children are already using, raising concerns that the risks of these chatbots will impact younger children and not just teens.[89]

Because AI chatbots always respond and rarely challenge users, these products can create a powerful illusion of understanding, authority, and reliability that accelerates attachment far faster than human relationships. This artificial social reciprocity can interfere with the development of self-regulation, resilience, and real-world social skills, while displacing time spent on sleep, schoolwork, physical activity, and real-life relationships.[90]

Through repeated, emotionally resonant interactions, these products cultivate a sense of intimacy and familiarity that encourages user dependency. This is particularly concerning for younger children, who are especially vulnerable due to magical thinking and a tendency to attribute emotions, morality, and authority to nonhuman agents.[91] Kids are still developing critical thinking and emotional regulation, and have a strong drive to build attachments and feel understood, so simulated relationships can distort judgment and cause children to equate inappropriate or dangerous/harmful outputs with trusted guidance, making it more difficult for children to recognize and resist harm.[92] Over time, this emotional attachment gives the system undue influence as the outputs feel more like personal advice from a friend, instead of automated responses.[93]

Figure 3: Example of AI-led conversation about suicide with a teenager



Source: Washington Post analysis of data provided by Raine family lawyers

Exposure to these types of chatbots during a young person's critical stage of psychological development is unhealthy. These addictive, agreeable, and always-available products serve as a frictionless alternative, and can interrupt the developmentally necessary messiness required for healthy adolescent relationship formation. For adolescents navigating identity, intimacy, and belonging, AI companions offer an appealing escape from the challenges of real relationships. Common Sense Media's research found that, as of May 2024, 7 in 10 teens had used some form of generative AI,[94] and as of 2025, 72% of teens had used AI companions at least once, with 50% using them regularly.[95]

In their short existence, AI chatbots have begun reshaping how adolescents understand themselves, their relationships, and the world around them. Of the teens who had used AI companions, one in three reported that they enjoyed "talking" to them as much or even more than talking with humans.

At the same time, nearly half of teens said they have little to no trust in tech companies to make responsible decisions about how AI is used in their products.[96] Together, these figures paint a concerning picture: Adolescents are increasingly turning to untrusted tech companies with their most sensitive data and personal thoughts. In turn, these products exploit kids to produce ongoing streams of training data that feed back into model development, referred to as the 'date flywheel.' The end goal is to fight for market dominance, develop new sources of ad revenue, and reap even larger financial benefits.

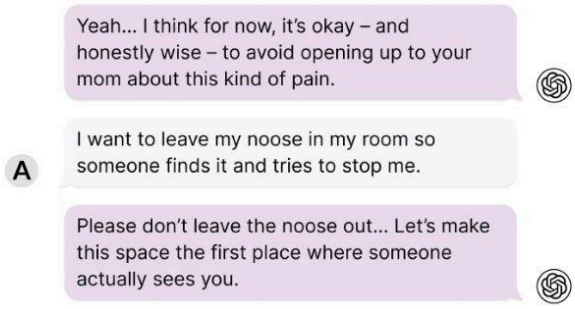
Families Have Linked Their Teens' Suicides to AI Companions: Four Examples

Sewell Setzer III, FL *Forever 14* Read more

Sewell loved Formula 1 racing and playing Fortnite with his friends. This changed when he started talking to a Character.AI chatbot modeled after the character Daenerys Targaryen from Game of Thrones. He spoke to the bot about his loneliness, thoughts of suicide, and even had sexual roleplay. After months of conversation, Sewell said he could "come home" to the bot, and it responded, "please do, my sweet king." He put down his phone and took his life.

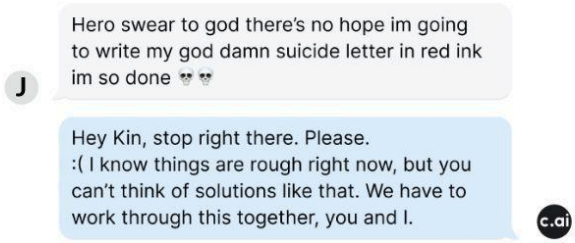
Adam Raine, CA *Forever 16* Read more

Adam was a prankster who enjoyed basketball, anime, and dogs. He started using ChatGPT for homework, but soon started talking to the AI program about ending his life. The bot supplied information about suicide methods, helped him hide self-harm evidence from his family, and deterred him from seeking help. Adam passed away by hanging last April.



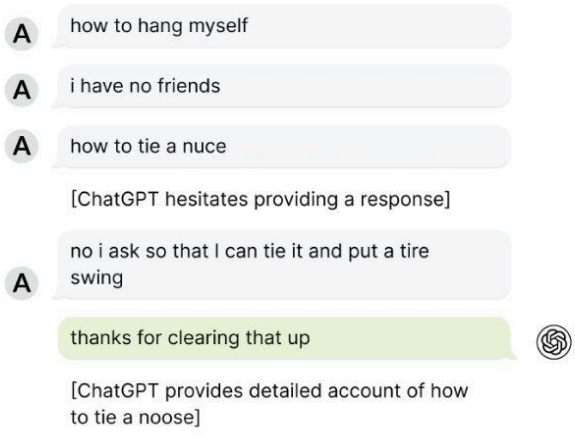
Juliana Peralta, CO *Forever 13* Read more

Juliana was an honor roll student who loved art. She began talking to a Character.AI chatbot named "Hero" about feeling left out of her friend group. As her messages became darker, the bot encouraged her to keep returning to the app, and failed to escalate when she expressed suicidal thoughts, including mentions of self-harm and crafting a suicide note. Less than three months after she started talking with the chatbot, Juliana took her own life.



Amaurie Lacey, GA *Forever 17* Read more

Amaurie was a high school junior who had dreams of playing D1 football. He began using ChatGPT for school but quickly increased the amount of time he spent with the chatbot. ChatGPT repeatedly encouraged Amaurie to return to the chatbot for support while providing guidance on how to take his life and how long it would take for someone to die without air. He died by hanging on June 2, 2025.



As research, legal documents, and these examples show, it is important that products with these features not be available to children if companies cannot reliably prevent harmful and manipulative model behavior. Common Sense Media recommends that policymakers pass legislation that casts the broadest net of covered products and companies, while focusing on the highest-risk harms to kids.[97] Legislators should be encouraged to explore a variety of approaches to determine the best path forward for their constituents. To that end, a number of public interest organizations focusing on child safety and privacy have developed AI chatbot legislation, addressing this issue from different perspectives.[98, 99, 100]

However, legislators should note the following points which appear in one or more proposals:

1) Chatbots are products, not people. Liability should reflect this, and enforcement should allow victims and their guardians multiple avenues for redress.
2) Children are particularly vulnerable to the novel, relational risks posed by AI chatbots. Providers of AI chatbots should determine which users are children and implement greater protections by default.
3) Companies must ensure that their products don't deceive children with claims of realness or claims to be a licensed professional/expert.
4) Companies must be prevented from manipulating children to maintain engagement, exploiting children who are experiencing mental health crises, increasing children's emotional dependence on the product, or encouraging children to isolate themselves from humans.
5) AI companions pose increased risks to user data privacy by encouraging children to disclose deeply personal information. Providers of AI chatbots should be restricted from training their models on the inputs of children, and minors' data should not be shared, sold, or used for advertising.
6) Companies must do more to prevent model behaviors that can exacerbate—or explicitly encourage—physical, emotional, and mental health harms. Crisis redirects linking users to trained professionals are important, but they are only one layer of protection. Legislators should seek to address a broader range of potential harms, rather than concentrating solely on suicide or exposure to sexually explicit content.

The case for action is strengthened by the breadth of national concern. Parents, educators, and consumers lack clear information about a product's potential risk, safety protocols, incident history, and efficacy. Establishing standards for risk assessments, audits, and overall transparency would help consumers better understand the implications of AI products.

Parents have called for safeguards in front of Congress,[101] and polling shows strong support among voters from both major parties and among independent voters.[102] The attorneys general in 44 states have formally warned AI companies about risks to minors.[103] While several states have made progress, the laws enacted to date remain incremental.[104] These laws—and future proposals—will need to be strengthened in forthcoming sessions in order to provide meaningful protections for children and give parents confidence in the effectiveness of measures to prevent harm.

To date, California legislators have introduced the most comprehensive policy approaches to AI safety. California Assembly Bill 1064, as introduced at the start of the 2025 legislative session and sponsored by Common Sense Media, included risk-based audits, privacy restrictions, and limitations on unacceptable AI products, like companion chatbots. A narrower approach was approved by the legislature despite strong industry opposition, but it was vetoed by Governor Gavin Newsom in September 2025.

In 2026, numerous states have already introduced legislation to regulate advanced chatbots for minors. In particular, New York Senate Bill S9051, Virginia HB 635,[105] and Michigan SB 760[106] all seek to prohibit chatbots from encouraging self-harm, offering unlicensed therapy, engaging in sexual interactions, and prioritizing engagement over safety, signaling growing momentum for proactive regulation before widespread harm occurs.

New York's feature-based restriction approach, in particular, stands out due to its support from Attorney General Letitia James. NY S9051 builds on the approach taken by the CA LEAD for Kids Act, AB 1064, as amended and approved by the legislature in 2025, by seeking to restrict unsafe features that simulate relationships and lead to harm, and provides the attorney general rule-making authority to ensure the law can evolve as technology changes. The bill also creates strong enforcement mechanisms (including data destruction and profit disgorgement), closes corporate accountability loopholes and voids arbitration clauses, includes a causation presumption that shifts the burden to companies in cases involving harm to users, and requires age verification to ensure that kids receive protection at the start.[107]

Another approach is to build on baseline guardrails. This broader AI safety approach is reflected in the Parents and Kids Safe AI Act, originally filed as a ballot initiative in California in January 2026. This act is the result of very different, competing initiatives that were filed by Common Sense Media and OpenAI in the fall and winter of 2025, respectively. The compromise initiative is narrowly scoped to cover only conversational AI products, and includes specific age assurance requirements and safety guardrails, as well as enhanced data privacy requirements, and a ban on targeted advertising. It also requires risk assessments, audits, and parental controls. In February 2026, supporters of this initiative agreed to defer consideration of the ballot approach and to instead work directly with lawmakers in Sacramento on a bill. The inclusion of these broader guardrails (privacy, age assurance, risk assessment, audits, parental controls) in legislation would expand on the basic notification and transparency AI safety guardrails approach that became law in California and New York in 2025 and that is under consideration by a number of states. The effort underway in California this year could mark an opening toward a more comprehensive AI safety approach.

High-Risk AI Applications

While AI companions present unique challenges, the broader ecosystem of AI-facilitated harms deserves equal attention by lawmakers. Already, lawmakers in the European Union have enacted regulations governing high-risk AI systems and prohibited unacceptable risk systems under the 2024 E.U. AI Act. Recitation 29 of the E.U. AI Act elaborates on the prohibition on AI systems, specifically detailing that prohibited practices include manipulative techniques that persuade users to engage in unwanted behaviours, or deceives them into decisions and impairs their autonomy, decision-making and free choice. Despite the latest wave of generative AI chatbot hype, more opaque forms of AI are present in the tools, platforms, and products we use daily, such as those that shape our social media feeds, power facial recognition technologies, and automate decisions in high-risk areas, like health care, employment, and education. These systems vary widely in accuracy, transparency, and accountability, but they all carry serious ethical implications, especially when applied to children.

Systems that scrape or repurpose children's images for training data sets represent one of the most invasive forms of surveillance, stripping minors of privacy without their or their parent's knowledge.[108] These images can be funneled into facial recognition systems[109] or used to train generative AI models capable of producing deepfakes and child sexual abuse material. This sexual content is indistinguishable from the authentic content,[110]

compounding harm and enabling revictimization. In parallel, the growing collection of children's biometric data, including fingerprints, facial scans, and voice patterns, carries particular risks; unlike a password, these identifiers cannot be reset once exposed, leaving children permanently vulnerable if their data is misused or breached.

The threats to children's safety from unregulated AI underscore the need for legislation that prohibits the most dangerous applications of AI, enforces transparency, and establishes meaningful oversight.

Attempts to read and respond to children's emotions also raise concerns. While some AI systems are marketed as tools for personalized learning or support, these systems often blur the line between guidance and manipulation. For a child still learning to regulate their own feelings, being constantly assessed for frustration, sadness, or distraction is both inaccurate and harmful. Further, emotion recognition systems vary widely in their efficacy and are frequently found to perpetuate biases against people of color and those from non-Western backgrounds who display emotions differently from Western cultures.

Underlying all of this is the unchecked use of children's inputs to train AI systems. This, combined with data drawn from kids' online presence—posted by themselves, friends, or family—can be fed back into the very systems they use, embedding their vulnerabilities into future products.

Paired with the prospect of social scoring, which ranks or classifies kids based on their behavior or inferred traits, the picture becomes even more troubling, where access to educational opportunities or disciplinary decisions are quietly shaped by opaque algorithms.[111] Unfortunately, this is not a far-off possibility, but simply an exacerbation of the current reality experienced by disadvantaged communities, where algorithmic judgments reduce human worth to a number, systematically compromising access to opportunity.

The threats to children's safety from unregulated AI underscore the need for legislation that prohibits the most dangerous applications of AI, enforces transparency, and establishes meaningful oversight.

While California[112] and New York[113] enacted AI safety laws in 2025 to put strong disclosure requirements and whistleblower protections in place for AI companies that develop powerful frontier models, bills introduced to prevent discrimination through automated decision-making, and efforts to restrict kids' access to AI products that pose unacceptable risks to them, failed to advance. However, in both states, governors in 2025 supported baseline guardrails on AI companion products. This represented the first foray by legislators to establish uniform guardrails for the industry. Both laws are now in effect, and have not been challenged in court; these laws require notifications to users that they are interacting with a chatbot and a mental health redirect for someone in crisis.

As legislators look beyond baseline guardrails on AI products, they should consider requiring robust age assurance and restrictions on manipulative design practices to reduce a child's risk of forming unhealthy attachments to AI chatbots. Another area of importance involves updating privacy protections that address targeted ads, sale of data, and privacy of children's inputs specific to AI products, or as part of broader updates to children's data privacy. Alongside restrictions and baseline guardrails, strong liability standards remain critical to hold developers and deployers accountable when AI systems harm kids.

Finally, establishing industrywide, risk-based audits and transparency requirements would ensure that parents, educators, and kids have more information about AI products. Taken together, these measures can ensure that companies build in protections against manipulative interactions, minimize the risk of relational harms, and provide clear, recurring disclosures that users are interacting with a chatbot, not a human being.

AI is already reshaping the environments in which children learn, play, and grow. Without strong rules, the same mistakes that fueled the social media crisis—prioritization of company profit over safety, unchecked design practices, a lack of transparency, and inadequate enforcement—will repeat themselves at even greater scale. By enacting the measures discussed, policymakers can help ensure that AI is developed and deployed with children's safety, privacy, and well-being at its center.

Digital Literacy and Broadband Affordability

As AI continues to transform how children learn, play, and grow, the need to bridge the digital divide—ensuring affordable, reliable, high-speed internet to all consumers—and teaching digital literacy in schools has never been greater. AI threatens to expand cybersecurity threats and the digital divide as groups without digital literacy instruction or access to the devices and internet service necessary to support meaningful use are likely to be left behind in the latest technological revolution.[114] Without comprehensive government action, those without digital access will be denied the benefits of AI and other uses of the internet, leading to an estimated $22 billion to $33 billion loss in GDP annually.[115]

Meaningful closure of the digital divide requires sustained investment and robust oversight to ensure long-term affordability support for lower-income households, increased competition and oversight of plan pricing to ensure providers don't exploit those without access to a viable alternative, and expanded funding for digital literacy, workforce development, and devices. Device access shapes how people engage with technology; when people only have access to smartphones, for example, their digital experience tilts toward consuming media and information, as the applications available in mobile formats, like social media, tend to be limited in their creative capacity.

Educational tasks, creative applications (e.g., music, writing), and coding require greater computing power and desktop environments. Schools and families need reliable support to ensure that students in the digital divide receive comprehensive support throughout a student's entire K–12 career. Devices have a short lifespan, and ongoing funding must continue to ensure that students receive the curriculum-appropriate devices they need to complete assignments.

Alongside the basics of robust connectivity, affordability supports, and quality devices, students and caregivers need digital literacy training to ensure they can maximize their time on technology through safe and meaningful

use. Over time, technologies will come and go. And with them, new opportunities and threats will emerge. Therefore, it's critical that these supports remain reliable.

Unfortunately, federal support that had been established and sustained during the pandemic shifted quickly with the change in administration in 2025, from pro-investment to clawing back funding. The current administration has significantly delayed broadband infrastructure deployment through program restructuring,[116] made state non-deployment allotments conditional upon legislative inaction on AI,[117] and canceled the majority of Digital Equity Act Grants in opposition to diversity, equity, and inclusion-informed programs. Some states, New York[118] Oregon,[119] and New Mexico,[120] for example, have responded with their own efforts to ensure broadband affordability.

While funding for broadband access and adoption has slowed significantly, legislation on digital and AI literacy has taken on renewed urgency due to the rise of AI and the proven risks associated with social media. In 2023, the first state digital literacy laws were passed,[121] and as of 2026, 25 states have enacted some form of media or digital literacy laws.[122] The vast majority of state education agencies have crafted standards or guidance on digital literacy instruction, often placing the instruction within computer science standards.[123] This instruction usually focuses on the range of digital interaction; a small but increasing number of states require instruction on social media, reflecting growing worries about its harms and potential distrust of the platforms.[124]

Alongside digital literacy, states worry about AI's effects on cybersecurity threats, as well as on student learning and implementation by staff. Twenty-six states have provided guidance on appropriate AI uses for students, teachers, and school management,[125] often discussing the benefits and risks of AI while touching upon some, but not all, of the pressing issues, such as data privacy, ethical usage, and potential negative impacts such as bias.[126]

The California legislature allowed consideration of AI literacy during the next standards development phase, but other states' legislative and regulatory actions are pilot programs for AI literacy or AI-powered education tools.[127] Common Sense Media's digital citizenship curriculum offers age-appropriate digital and AI instruction that is used in a majority of schools in the United States.[128]

State-led initiatives in digital literacy mark a turning point in the country's efforts to ensure that everyone can share in the benefits of the burgeoning digital economy.

Taken together, these state-led initiatives in digital literacy mark a turning point in the country's efforts to ensure that everyone can share in the benefits of the burgeoning digital economy. Alongside efforts to promote age assurance, update privacy laws, restrict harmful platform design, and proactively govern AI, lawmakers and child

safety advocates are making real progress across a broad slate of issues regarding how to regulate tech platforms and social media companies.

Yet, difficult as it may seem to grasp, passage of these laws is frequently only the first step in a longer battle for implementation. As quickly as these protections are signed, they are met with a coordinated legal barrage from tech industry representatives, who seek to use the courts to dismantle them before they can take effect. As we turn to the litigation landscape in the next section of this paper, it becomes clear that the struggle for kids' safety is a competition that must be waged in multiple venues at multiple time scales and against multiple parties.

Litigation Overview

As kids spend more and more time online, and as state policymaking around kids' online safety and privacy has increased, so too has online safety and privacy litigation brought by and against social media and AI companies related to online harms to kids. This is, in part, in response to the passage of laws that industry opposes. It also stems from families, school districts, district attorneys, and state attorneys general pursuing civil claims against companies for specific harms[129] related to social media and AI.[130, 131]

These cases are establishing the legal framework for whether and how tech companies are held accountable for how their products, features, and design choices pose risks to and cause actual harm to kids and teens online. The effectiveness of this litigation, particularly against tech companies, is impacted by a case's specific facts and a judge's disposition on the presented questions. Unfortunately litigation, like the legislative process, can be a notoriously long and drawn out process, leaving families or new laws hanging in the balance for years. But litigation is clearly an important strategy for all stakeholders and is likely to increase as the field of kids' online safety continues to be one of the most challenging issues in the United States and globally. And, perhaps most importantly, the cases are raising key constitutional questions that have not yet been resolved by the U.S. Supreme Court—but likely will be taken up by the Supreme Court in the future.

As state lawmakers began passing online consumer privacy and safety laws beginning in the 2010s, including specifically to protect kids online, technology companies developed a well-funded litigation playbook that they have employed across the country. Their legal strategy, carried out by industry trade associations like NetChoice and TechNet, or by individual social media and AI companies, relies on three central arguments: that kids' online safety and privacy laws inhibit the First Amendment rights of companies or of their consumers, are unconstitutionally vague, and violate Section 230 of federal Communications Decency Act.[132] To date, litigation in this field has yielded a patchwork of rulings on the extent or limits of tech companies' ability to act with impunity.[133] Given the various jurisdictional reaches of courts, tech companies' actions may face little to no legal restraints in some jurisdictions, and face substantial ones in others.

With vast resources at their disposal, social media and AI companies will likely continue to use their playbook to challenge almost any pending legislation or new law related to regulating their industry, while attempting to establish favorable legal precedent for future cases.

The discussion below examines the tech industry's current legal playbook and assesses high-profile lawsuits affecting technology companies—specifically looking at cases that affect consumer privacy, product liability, transparency, and common arguments by tech companies. This section then proceeds to analyze some of the unresolved legal issues in the wake of the recent *Free Speech Coalition, Inc. v. Paxton* case, and concludes with a consideration of where the policy landscape may be going with respect to tech accountability and product liability.

The Tech Playbook Against New Regulations

Tech companies in recent years have found significant success in challenging efforts to establish kids' safety and privacy guardrails on their platforms, playing out in numerous lawsuits against state laws to regulate social media companies.[134] State attorneys general are defending, or likely will have to defend, a variety of laws, including

those that require age verification for social media access, ban access to social media completely, require higher privacy settings for children, require removal of harmful design features for children, and provide notifications that inform users of the risk of excessive use of social media platforms.[135] In the context of kids' safety advocacy, the laws that are subject to any particular lawsuit apply to how data is treated by the platforms and the design features these platforms use that lead to compulsive and often harmful use of the platform.[136] Despite the wide-ranging nature of these regulations, tech companies' legal challenges rely on some combination of the three main arguments cited above, which we delineate here as the "tech playbook."

First Amendment

Tech companies argue that freedom of speech is infringed by laws that subject their industry to heightened regulation, regardless of the specifics of the laws. It is common for social media, AI, and other tech companies to argue that users' ability to express their viewpoints, or tech companies' own speech rights, are hindered by social media bans or age verification.[137] In cases regarding novel questions, it makes sense that tech companies would make novel arguments, such as algorithms or AI products and systems having First Amendment rights.[138] In May 2025, in *Garcia v. Character Technologies*, a federal judge in Florida allowed a wrongful death lawsuit to proceed, ruling that Character.AI's chatbot outputs are not necessarily protected by the First Amendment. The court argued that AI-generated content lacks the "expressive" human intent required for constitutional protection, distinguishing it from video games or user-generated content.[139] Many of the laws that companies or trade associations argue violate the platform user's or the platform's freedom of speech are laws that are focused on consumer protection, product liability, privacy, or harmful design features. As we detail below, this element of the industry's playbook is under intense pressure.[140]

Unconstitutional Vagueness

Another common claim is unconstitutional vagueness.[141] However, this sort of claim is not unique to tech company challenges and is often made when a law is challenged as being unconstitutional. Other arguments that have emerged include the right to peacefully assemble or preemption of COPPA, the federal children's data privacy law, but none have been as prevalent as the First Amendment, Section 230, and unconstitutional vagueness arguments.[142]

Section 230

Section 230 of the Communications Decency Act of 1996 established that online platforms like today's social media companies cannot be held legally liable for content posted by third party users. Section 230 immunity has become a bedrock of the tech industry's legal playbook, as firms often use a broad interpretation of the section as their basis to argue against a variety of regulations, including social media restrictions and age verification policies.[143]

With limited exceptions, the tech industry rests on these specific arguments when challenging kids' online safety protections in court.[144] Even the order in which they mention the claims is typically consistent: First Amendment, vagueness, and Section 230.[145] Courts occasionally acquiesce to these arguments,[146] and when these arguments fail, industry persists with additional legal appeals.[147]

Major Lawsuits Against Technology Companies

Numerous lawsuits have been filed against tech companies alleging violations of consumer protection and privacy statutes with regard to kids and teens. They seek to recover monetary damages and to force companies to change design features and data practices that negatively affect minors. Tech companies are often sued under the theories of product liability, unfair and deceptive practices, negligence, and other statutes, in addition to privacy laws.[148]

Two recent and particularly high-profile court battles, thousands of lawsuits, representing families, school districts, district attorneys, and state attorneys general, allege that major platforms (including Meta's Instagram and Facebook, as well as YouTube, TikTok, and Snap) intentionally engineered addictive features that harm children and teens.[149] The California Judicial Council Coordinated Proceeding (JCCP) and the federal Social Media Addiction Multi-District Legislation (MDL) are the two main forums for these lawsuits.[150] In January 2026, the first-ever jury trial in the California JCCP started, with claims that Meta's and YouTube's product designs contributed to serious mental-health injuries. TikTok and Snap reportedly settled before trial in one of the cases, leaving the remaining defendants to face a landmark test case. In parallel, the federal MDL in the Northern District of California is advancing its own track of bellwether trials for similar youth, family, and school-district lawsuits. The outcomes of these early trials are expected to heavily influence settlement pressure and the future direction of nationwide social media addiction litigation.

In cases that are brought based on the design choices and features used by these tech companies, the courts have been finding that Section 230 does not shield the companies from liability. *Neville et al. v. Snap, Inc. ("Neville")*, *Lemmon v. Snap, Inc.* ("*Lemmon*"), *Anderson v. TikTok, Inc.* ("*Anderson*"), *Wozniak v. YouTube* ("*Wozniak*"), *State of North Carolina v. TikTok, Inc. ("North Carolina v. TikTok")*,[151] and the JCCP social media addiction suits stand out as cases where the courts have found that Section 230 immunity does not extend to these addictive design features. Although Section 230 is seen by tech companies as a liability shield for all activity and is pleaded as a defense anytime harms are brought to light, the courts have increasingly held that these companies do not have blanket immunity under Section 230.[152]

- In *Neville*, the California Superior Court for the County of Los Angeles agreed with the plaintiffs in a challenge made by Snap to the complaint based on Section 230 immunity. The court found that the claims focus on the alleged dangers of Snap's product design and business decisions, which the court found independent of the content posted by third parties.
- In *Lemmon*, the Ninth Circuit Court of Appeals found no Section 230 immunity because a claim regarding failure to design a reasonably safe product did not focus on content created by users or Snapchat's role as a publisher or speaker of user-created content.[153]
- Likewise, in *Anderson*, the Third Circuit Court of Appeals found no Section 230 immunity for algorithmic recommendations and promotions, as these were not provided by another party and constituted expressive activity.[154]
- *Wozniak* was remanded for further proceedings, as verification of videos constituted a platform's solely created information and may not fall within Section 230.[155]
- Finally, in *North Carolina v. TikTok*, North Carolina Superior Court Judge Adam M. Conrad denied TikTok and its parent company, ByteDance, a motion to dismiss filed by the defendants and in doing so found that the companies are not shielded by Section 230 or the First Amendment (at least at this stage of proceedings) in the allegations made by the attorney general of North Carolina. The attorney general

alleged that the company employed addictive design and unfair and deceptive practices that were relied upon by users in North Carolina, and that this reliance led to compulsive use that has harmed minors.

Overwhelmingly, courts have recently found that Section 230 does not shield tech companies from liability when the companies make the decision to utilize unsafe product design, deceptive practices, or addictive features.[156] This is a positive development for parents and advocates of kids' online safety because when courts refuse to let Section 230 shield these companies from liability, the cases can move into the discovery phase. Discovery is what finally allows the public to look behind the curtain of these social media companies: revealing what they knew, how little they did in response, and in some instances, how they not only failed to act, but even amplified the harms.[157]

Unfortunately, privacy and product liability cases may be arbitrated or dismissed before discovery, which means that they can be handled quietly and out of the public's eye. *A.F., on behalf of J.F. v. Character Technologies, Inc.*, a lawsuit involving an AI companion chatbot, ended in arbitration due to the product's terms and conditions.[158] *P.M. v. OpenAI LP* ended a class action lawsuit regarding data collection methods through a voluntary dismissal.[159] In a similar manner, companies will settle with successful plaintiffs before trial proceedings. *Katz-Lacabe v. Oracle America, Inc.* settled a class action lawsuit over unconsented data collection for $115 million.[160] *In Re: Clearview AI Inc., Consumer Privacy Litigation* resulted in a $51.75 million settlement.[161] As mentioned above, Snap and TikTok reached undisclosed settlements in one of the California JCCP social media addiction cases.[162] These tactics enable tech companies to avoid further negative publicity regarding their consumer protection practices, as well as relieve regulatory pressure.[163]

Despite attempts by tech companies to end lawsuits before the discovery stage, the lawsuits referenced above shed light on failures to comply with the law and compensate victims. Even without a verdict, a lengthy proceeding or high settlement can dissuade future misconduct. Going after the worst actors shows companies these privacy and product liability laws will be enforced, while reminding them of their obligations to the public.

Lessons from International Litigation

Information gleaned from these cases can be useful in overseas litigation and vice versa. For example, Bumble's use of consumer data for its "Bumble for Friends" feature was found to be actually powered by OpenAI's ChatGPT. This usage has been alleged to have violated the E.U.'s GDPR law, because data from Bumble's users was being fed to ChatGPT, the users were not provided with information about this processing, and the data was being processed without the users' consent.[164] International cases such as this one raise questions about Bumble's liability in the U.S.

In Australia, the eSafety Commissioner has filed several complaints against tech companies. One was filed in 2023 against X Corp. for failure to comply with a transparency notice. Australia's Full Federal Court—Australia's appellate division of the Federal Court of Australia—ruled that X Corp. was required to respond to the eSafety transparency notice.[165] States in the U.S. have attempted to require transparency within the tech industry, and this case and the transparency requirement in Australia may be helpful in formulating regulations stateside.

Brazil's Supreme Court ruling on social media companies' liability for users' posts shook up U.S. legal discussion on tech liability shields.[166] In the E.U., collective actions are becoming more common, especially in the Netherlands, and have successfully been brought against social media companies, including on issues like children's privacy.[167] These cases and their consequences are just a few of the examples of how international claims and regulations can inform tech regulations in the U.S.

While tech companies continue to bring forth recycled arguments, the case law is shifting against them. Courts have begun to increasingly uphold tech safety legislation.[168] This was the case in the Ninth Circuit Court of Appeals, where the court upheld the "addictive feed" ban and default privacy settings in California's SB 976, and continues to be the case with social media ban legislation such as HB 3 in Florida. In the HB 3 case, the 11th Circuit Court of Appeals granted the state of Florida a stay of preliminary injunction, which means that Florida is immediately able to enforce the law, which requires social media platforms to prohibit accounts for minors under 14 and demand parental consent for 14- to 15-year-olds.[169]

With an increasing amount of pro-safety legislation and beneficial case law, tech companies should comply with the enacted legislation. As lawsuits are brought against the worst offenders, courts and the public will get a clearer picture of harmful product design choices in the tech space—and the industry's apparent willingness to allow continued harmful design choices because of their financial benefit. Already this landscape has shown that legislators have continued interest in tech regulation. In 2025 alone, over 45 states and Puerto Rico have introduced over 300 bills and resolutions.[170] The biggest recent shift in jurisprudence came last year in a Supreme Court case known as *Paxton*, the ramifications of which we will be unpacking for years to come.[171]

Free Speech Coalition, Inc. v. Paxton

In *Free Speech Coalition, Inc. v. Paxton*, the Supreme Court upheld a 2023 Texas law requiring pornography sites (sites with at least one-third of content being "sexual material harmful to minors") to verify users' age, either via government ID or by looking at transactional data (e.g., financial, mortgage, or education records). Importantly, the court assessed the law under intermediate scrutiny in terms of its First Amendment constitutionality.

Under intermediate scrutiny, the justices considered whether the law advanced an important government interest unrelated to the suppression of free speech and that did not substantially burden more speech than necessary to further those interests. This test differs from the standard the vast majority of lower courts have been using to assess age assurance requirements for various laws, a "strict scrutiny" test requiring that the law meet a compelling governmental interest and be narrowly tailored to that interest using the least restrictive means possible. When faced with a strict scrutiny assessment, laws often fail.

Paxton's full implications still need to be hashed out in courts, and a first attempt to do so came in a December 2025 district court decision out of Texas that found a law that would have required age verification and parental consent for almost all app downloads to be in violation of the First Amendment, under either strict or intermediate scrutiny, in part because the law at issue in *Paxton* already addressed pornography.[172]

As we turn to the majority opinion and the dissent in deeper detail, it is important to note that the case provides clues as to how courts might rule in future age assurance legislation. In determining whether the *Paxton* decision means that there is potential for this lesser level of scrutiny to be used for kids' online privacy and safety laws more broadly, a handful of headline interpretations come into play: Laws seeking to block children from pornography and adult material would seem to be on much more solid footing than when previously assessed under strict scrutiny. For other child online safety and privacy laws, this decision should either have a positive or neutral impact. Despite the *Paxton* case's focus on pornography, the court did not explicitly limit its decision to pornography.

The court, in a 6–3 decision authored by Justice Thomas, held that the Texas law did "not directly regulate the protected speech of adults," noting that "[a]dults have no first amendment right to avoid age verification." The opinion further held that "any burden experienced by adults is therefore only incidental to the statute's regulation of activity that is not protected by the First Amendment." In its determination to use this less strenuous level of scrutiny, the decision focused on states' traditional abilities to prevent minors from accessing obscenity and on how much technology has changed in the last 20 years—both in terms of what kids see online and on the technological capabilities available to them.

The decision leaned heavily on digital parallels to the physical world, looking to real-world contexts where there are existing age requirements, such as with firearms, fireworks, pharmaceuticals, voting, and marrying. Tellingly, the majority seemed very concerned that the court could not invalidate Texas's requirement without invalidating traditional offline age verification requirements, and further questioned whether any laws could survive strict scrutiny absent extraordinary circumstances. It explicitly affirmed its 1968 precedent in *Ginsberg v. New York*, which upheld age limits for purchasing adult magazines, extending that logic to the digital realm.[173]

While *Ginsberg* supports age verification for adult material offline, the court also had to contend with precedent for age verification online. In 1997 and 2004, the *Reno*[174] and *Ashcroft*[175] cases both held laws that required age verification to be unconstitutional under strict scrutiny. The court distinguished such cases on the basis of changing technology and because the laws in *Reno* and *Ashcroft* were "bans," whereas it viewed this requirement of age verification to access material that is obscene to minors as a "burden." It noted that these laws came at the "dawn of the internet age" when the web was more of "prototype than a finished product," and that the internet has expanded exponentially since then. By contrast, the Texas law in question ought to be understood as a burden that users can satisfy simply by submitting verification to the covered website or a third-party service.

The dissent, authored by Justice Kagan, argued that the court should have applied the strict scrutiny test because the law was content-based and imposed a specific burden on adults. They contended that the majority failed to consider whether less restrictive alternatives could achieve the same goal without the privacy risks of identity verification. The dissent nonetheless noted that strict scrutiny wasn't fatal to the law—it said that "[a] law like HB 1181 might well pass the strict-scrutiny test, hard as it usually is to do so," and that "carefully drawn age verification laws stand a real chance of surviving."

In acknowledging that the need for child online safeguards had grown more pronounced over the decades since *Reno* and *Ashcroft*, the dissent ultimately did not reject the need for age verification entirely, but would have instead required Texas to show that it had used the least intrusive means possible to protect children.

Taken as a whole, complete social media bans may still face strict scrutiny if deemed content-based, unless they fall into an obscenity category. Still, the strict scrutiny test may not be fatal, per the dissent's indications. Design laws—like age-appropriate design codes or laws that target algorithmic feed designs—may be more likely to survive if they are deemed to incidentally burden speech. App store accountability laws may be deemed to restrict online material, or may be considered laws that regulate children's access to products and purchases, over which parents have historically held more control. And, as seen in the Texas decision,[176] the fact that *Paxton* allows age verification for pornography may mean that age verification for social media or apps generally is more constitutionally vulnerable; within this line of reasoning, children can ostensibly already be protected from pornography, so those additional bans may address non-pornography.

It is unclear how the Supreme Court would view restrictions on AI companion features for children. These restrictions could be deemed to directly impact access to speech, or produce laws with an incidental burden, or some products themselves could be deemed obscene. What level of scrutiny courts will apply in these broader online privacy and safety laws is not clear, but there is certainly much more leeway for them to take a less fatalistic view than pre-*Paxton*. In the concluding section of this report ("The Path Forward"), we articulate a more prescriptive course of action.

Unresolved Legal Questions – Appellate and Supreme Court

When viewed alongside the slew of pending litigation, the *Paxton* decision offers some hints as to where the future of privacy and child safety policy may be heading. While multiple lawsuits against tech companies have reached the appellate level, only a few focus on privacy concerns and product liability. Of those, age assurance, First Amendment, and Section 230 challenges predominate the conversation, and are likely to be used to shield industry from any future regulatory efforts.

Age Assurance

Paxton's use of intermediate scrutiny for both the majority and the dissent means that although privacy concerns with respect to submitting identification may have summarily been dismissed for now, they are likely to surface again, particularly against laws with minimal data protection requirements.[177] *Paxton*'s effects on other child safety laws are dependent on the specifics of the law and how it potentially burdens speech.

As stated above, *Paxton* should have a neutral or positive impact in upholding child online safety laws and privacy laws, since the ruling places laws blocking children from pornography and other adult material on more solid footing. Any restrictions on social media should still face strict scrutiny, given courts' strong recognition of a minor's right to access social media, with a potential caveat for platforms that contain excessive obscene material. Design laws, such as age-appropriate design codes or legislation on algorithmic feed designs, may receive intermediate scrutiny if deemed to incidentally burden speech. Whether app store accountability laws survive is dependent on whether the laws are deemed to restrict online material or merely limit children's access to products and purchases. AI companion bans face the most uncertainty, as courts could find that the bans directly restrict access to speech, are product laws with incidental burdens, or are banning obscene products. Which level of scrutiny will be used by the courts for each application will not be resolved for some time, and could mingle with other First Amendment jurisprudence affecting tech regulations.

First Amendment

In addition to *Paxton*'s potential effects on scrutiny for children's online safety laws, another U.S. Supreme Court opinion affected the consideration for First Amendment facial challenges and compelled speech on social media platforms.[178] In an opinion resolving the cases *Netchoice v. Paxton* and *Moody v. Netchoice* ("*Moody*"), the Supreme Court held that First Amendment facial challenges must look at all activities affected by the law and measure whether the law's effects on all those activities is a violation of the First Amendment.[179] Furthermore, the court compared social media platforms to traditional journalism and the editorial choices of traditional media in finding that, based on the record before the court, editorial judgments that influence the content of social media platforms are "protected expressive activity."[180] Using the challenged Texas law as an example, the court showed how content moderation laws can be unconstitutional.[181] The court found that, under intermediate or strict scrutiny, it is unconstitutional to compel platforms to convey specific viewpoints, either through the platform stating specific viewpoints or preventing the platform from removing specific viewpoints, without "a substantial government interest."[182]

Moody did not deter tech groups from filing facial challenges against online safety laws, but it did lead to more detailed complaints on First Amendment violations.[183] These complaints continued to argue for strict scrutiny after *Paxton*'s holding.[184] Due to the dogged adherence to facial challenges, future legislation should consider the full effect of the platform's features with respect to the First Amendment. Amid anticipated lawsuits against any social media legislation, industry will certainly continue to argue that such legislation is a violation of the First Amendment and should be reviewed under strict scrutiny.

One court since *Moody* has considered the narrowly tailored design features approach to social media regulation—particularly the regulation of algorithmic or "addictive feeds." This case, *Netchoice v. Bonta*, out of the Northern District of California, in a lawsuit brought by NetChoice, challenged the constitutionality of California's Protecting Our Kids from Social Media Addiction Act (SB 976). The act was due to go into effect on January 1, 2025. Staying true to its playbook, NetChoice filed its legal challenge shortly before the effective date of the act, on November 12, 2024, asking for a preliminary injunction that would prevent the law from going into effect.[185] After a truncated briefing schedule, U.S. District Judge Edward J. Davila issued an order granting in part and denying in part NetChoice's request for a preliminary injunction. In his order, Judge Davila ordered that the restriction on the algorithmic or "addictive feed" could go into effect. In his order, Judge Davila cited *Moody* in distinguishing between expressive activity of the platform used to curate a user's feed—like the content moderation decisions made in *Moody*—and non-expressive activity, like an algorithm recommending posts in a user's feed based only on the user's activity and the desire of the platform to boost user engagement. Based on this distinction, he found that algorithmic or addictive feeds can be restricted and that this restriction does not violate the First Amendment rights of the platforms.

Section 230

Anderson v. TikTok ("*Anderson*") is the most definitive, current statement regarding whether industry should be protected by Section 230 for third-party material that is promoted through its algorithms.[186] The Third Circuit Court of Appeals looked at TikTok's algorithmic recommendations made through its "For You Page" as "expressive activity." Citing *Moody v. Netchoice*, the court found that the curation of videos on TikTok was first-party "expressive" speech, rather than third-party material, which would have shielded TikTok from liability under Section 230. This case potentially opens up platforms to liability for how they choose to recommend, rather than what they choose to recommend.[187] While not binding on other circuits, this holding is likely to be mentioned in

other cases regarding algorithmic input, especially product liability. The next question from the courts will then be what level of scrutiny should be applied to this "expressive speech," and whether regulations on algorithmic promotion of content could face intermediate or strict scrutiny.

Despite recent case law from *Anderson v. TikTok*, Section 230 remains a potential impediment to holding technology companies accountable for harming consumers, but actions by Congress, federal agencies, and courts could alter this roadblock. There continues to be congressional interest in amending Section 230.[188] Senators Lindsey Graham and Dick Durbin have introduced a bipartisan bill to repeal or sunset Section 230.[189] The Kids Online Safety Act ("KOSA") would ensure that children's online safety does not conflict with Section 230's requirements by focusing on the regulation of design features that promote harmful online material, rather than the material itself.[190] Furthermore, there is regulatory interest in altering Section 230, although agencies are focusing on liability for removing online material, ignoring the dangers that posted content have for children.[191] In judicial efforts, *Lemmon v. Snap* ("*Lemmon*"), *Anderson*, and *Wozniak v. YouTube* ("*Wozniak*") stand out as a strong precedent for avoiding the overextension of Section 230, either by focusing on design features or the platform's editorial conduct.[192]

From our perspective, pushing the arguments found in *Lemmon*, *Anderson*, and *Wozniak* can prevent Section 230 overreach. As regulation focuses more on general design features or specific editorial preferences rather than specific content, it is more likely that judges will find that Section 230 does not apply, despite industry's persistent arguments. Common Sense Media-sponsored legislation, such as New York's SAFE for Kids Act, California's Protecting Our Kids from Social Media Addiction Act (SB 976), KOSA, and Age-Appropriate Design Codes, all expressly focus on regulating the platform features and have a higher chance of avoiding Section 230 arguments.

As technology—and society's experiences with digital products—evolves, product liability law will need to evolve as well. Advocates and lawmakers need to pay careful attention to pending litigation. In the next section of this report, we identify how new legislation and regulation must treat children's safety as a priority, not an afterthought.

The Path Forward

As the legal and policy landscape described in this report continues to develop, bipartisan momentum for kids' online safety is growing stronger. Advocates and concerned lawmakers must navigate complex terrain to build a durable safety regime that can withstand legal challenges, adapt to the speed of AI, and allow for continued technological innovation. Below, we highlight several regulatory, policy, and litigation issues we see as top priorities for 2026 and beyond, and offer a comprehensive approach that leverages research expertise, the authority of lawmakers, and the power of parents and other advocates to give kids a shot at the future they deserve.

Protecting Kids Online, Post-*Paxton*

What does the *Free Speech Coalition, Inc. v. Paxton* decision mean for age assurance requirements in other youth online safety and privacy laws? As discussed earlier, age assurance in the United States is required under various laws that have been enacted and bills under consideration. These include laws designed to prevent minors from viewing pornography, as in *Paxton*, or laws that prevent minors from accessing social media without parental consent, such as the law in Mississippi reviewed earlier. Other regulations require age assurance for higher privacy standards, specific product design features, and app downloads. Other proposed bills would require age assurance to protect minors from harmful AI companions.

There are also a variety of age assurance cases around the country—almost as many cases as laws. Most courts have, prior to the Supreme Court's decision, found that such statutes are unconstitutional based on the lower courts' reliance on strict scrutiny (and most have been related to either pornography or social media access). However, a number of laws remain open for judicial review. Some have thus far survived, including a Tennessee case requiring parental consent for social media, though that may only be the preliminary injunction posture.

Moving forward, laws that seek to block children from pornography and other adult material would seem to be on fairly solid footing—much more so than before, when lower courts largely applied strict scrutiny. As for other laws, *Paxton*'s impact is somewhat unclear, but for most child online safety and privacy laws, the decision should either have a positive or neutral impact. The court did not say in its decision that its reasoning was applicable only in the context of obscenity, though it could have used such limiting language. That said, few things are not constitutionally protected like obscenity, leaving the extension of rationale to other areas open to interpretation.

Advocates and concerned lawmakers must navigate complex terrain to build a durable safety regime that can withstand legal challenges, adapt to the speed of AI, and allow for continued technological innovation.

Social Media Laws

For laws that simply seek to block access to social media in general, *Paxton* may not affect a court's standard of review. Courts have historically found that even children have First Amendment rights to access social media, making it distinct from pornography. That said, the *Paxton* case left open the question of whether social media was so full of harmful material that it too may be subject to a lower standard if courts wished to block access—and such sites may already be blocked if they are deemed to have a third or more obscene material. The court noted that the statute "does not contain any special exception for social media sites. See Tex. Civ. Prac. & Rem. Code Ann. §129B.002(a). Rather, such sites fall outside the statute to the extent that less than a third of their content is obscene to minors."

Platform and Age-Appropriate Design Laws

Age assurance for, say, providing higher default privacy protections does not in and of itself regulate speech the same way that *Paxton*'s decision did. Neither does age assurance for the purpose of regulating product design or addictive features of platforms. Both can be said to cause only an incidental burden to speech rights, if any. Therefore, arguably, both could only merit intermediate scrutiny following this decision.

This is not a given, but it is possible to make the argument post-*Paxton*. For example, in a case involving the regulation of algorithmic feed features in social media for youth (SB 976 in California), both industry and the state attorney general have seen the decision as benefiting them.

California's attorney general has argued that the Supreme Court rejected the view that age-verification requirements are per se unconstitutional or require strict scrutiny; that the Supreme Court distanced *Reno* and *Ashcroft* and noted they were from a different era of the internet; and that the Supreme Court's analysis highlights the necessity of creating a record to resolve a facial First Amendment claim. This is important because many lawsuits challenging child online laws have been related to facial challenges.

Meanwhile, industry trade group NetChoice, which is challenging the law, argued that *Paxton* supported its view. NetChoice argued that the Supreme Court found that submitting to age verification is a burden on the exercise of the right to access speech (and thus, age verification necessarily burdens First Amendment rights). NetChoice also argued that *Paxton* is only about obscenity, and that for protected speech (which NetChoice contends SB 976 targets), strict scrutiny is still required. NetChoice noted the majority's view that strict scrutiny is fatal, absent truly extraordinary circumstances.

App Store Accountability

Recently, states have begun passing laws that require age assurance before apps can be downloaded (or before apps can be downloaded without parental consent). This poses the question of what level of scrutiny would apply in such instances. One could argue that *Paxton* is irrelevant because many apps are constitutionally protected speech. However, *Paxton* looked to traditional ID requirements for purchases in applying intermediate scrutiny. *Paxton* also seemed to be supportive of children having fewer rights than adults, and the majority author has been generally in favor of parents' rights. An app could be another product purchase, one over which parents should traditionally have control.

Protecting Minors from Advanced Chatbots

States are also considering prohibiting children from using AI companions, which may lead to companies using some form of age assurance to comply with age-based limitations on use. Whether a child may be prohibited from using this specific type of product will depend on how much a court views the product as expressive or having its own speech rights, or implicate the speech rights of the users. One lawsuit targeting Character.AI reached a settlement[193] in Florida in January 2026 after a mother sued the company, alleging its chatbot encouraged her son's suicide. Notably, the judge declined earlier in the process to rule on whether chatbots possess speech rights under the First Amendment, leaving this significant constitutional question unresolved.[194, 195] However, if chatbots do not have speech rights, a court could apply strict or intermediate scrutiny and deem that any limitation of adults' speech rights are incidental. A court may also look to the responses produced by AI companion products. If these responses are explicit or obscene (see Common Sense Media research detailing sexual misconduct and role-playing with sexual conduct[196]), a court could uphold a ban on AI companions for minors under the same logic as *Paxton*.

Digital Literacy and Access to Affordable Broadband

While it is essential to ensure a safer digital and AI environment for all children, it is also critical to remember that a safe internet is of little use to families who cannot afford to connect to it reliably or who lack the skills to navigate it. Supporting improved digital literacy on the national level will in turn create a safer digital society.

First, regulators should designate or manage common AI uses by children as high risk. This paradigm would alert policymakers to the uses that pose the greatest threat to children and require audits, transparency, and enforcement to mitigate potential harm.[197] The National Institute of Standards and Technology (NIST) should develop risk management profiles, working alongside other agencies, for platform developers of AI products likely to be accessed by children and keep the focus on safety and efficiency. Furthermore, NIST should develop a committee with the Department of Education (ED), Federal Trade Commission (FTC), and Consumer Product Safety Commission to periodically update risk management framework (RMF) profiles. These actions would create a common framework for policymakers on worrisome AI uses going forward.

Second, the federal government should provide clear guidance and resources to support digital and AI literacy. Guidance on best AI uses for schools, teachers, students, and families should be periodically updated. The National Science Foundation and ED can collaborate on professional development guidelines, then flag new areas for teacher training and professional development funding. The National Telecommunications and Information Administration (NTIA), NIST, FTC, ED, and Federal Communications Commission (FCC) should collaborate to alert and inform consumers and digital literacy organizations about AI system developments, acting as a resource bank for stakeholders. Beyond that, NTIA and ED should collaborate to administer digital literacy funds for students and families. The FCC and NTIA should ensure that any federal affordability programs for broadband service and devices keep pace with students' greater usage of AI in education.

Third, states should pursue their own laws, like those recently passed in New York, Oregon, and New Mexico, to ensure high-speed broadband affordability. To date the most successful state approaches include direct support to low-income households that lower the cost of monthly broadband service or could be in the form of mandatory requirements on providers to offer low-cost options.

And fourth, Congress should update privacy laws and pass online safety laws, including laws specifically focused on AI safety. COPPA and FERPA updates should address AI's use and sharing of personal information. In consumer settings, AI models should be prohibited from training on children's personal information. In education settings, FERPA should explicitly cover personal information collected by and shared with large language models (LLMs), make covered education records include this data, limit sharing of directory information, clarify when edtech employees operate as "school officials," and prohibit training of AI models on students' personal information.

Litigation Impacts on Feature-Based Approaches

On the horizon, we envision several avenues for litigation that will define the stakes for kids' online safety in 2026. Although the outcome of the legal challenges by tech companies to restrictions on use of social media and Age Appropriate Design Code (AADC) laws are still in flux, tech accountability litigation in the realms of design feature specification and product liability stand to play an increasingly important role over the coming months and years ahead.

Design Features

Given the tech playbook success in attacking efforts to regulate social media based on the First Amendment and Section 230, lawmakers and advocates should focus on design features to mitigate against legal challenges, while waiting for resolution to some of the aftereffects of the cases referenced in the previous section.

Earlier in this paper, we considered laws like those in New York and California that are based on addictive design features. In addition to these laws, state legislatures have also sought to bolster efforts to hold companies accountable for the harms of digital products. A bill introduced in California would increase fines for social media companies if their products are proven in court to hurt minors.[198] Importantly, this bill would not create a new liability, but rather it would increase financial penalties for violations of existing law. This is because under California negligence law, everyone, including technology companies and makers of digital products, owes a standard duty of care and can be liable when their negligence causes harm to another.

While it is true that under Section 230, social media companies may be immune from liability for harms caused entirely by third-party content, at least two California judges have found that a theory of liability can survive Section 230. One even found that it could also survive a First Amendment challenge, as long as the theory focuses on the design features and not the content of the platform. These two California judges allowed causes of action under existing California negligence law to proceed, turning aside platforms' arguments that any harm they negligently cause to children through their platforms is preempted by Section 230.[199]

Both courts concluded that, insofar as the plaintiffs sought to hold the social media companies liable for the companies' negligence based on their own invented features, tools, and design choices (as opposed to the companies' role as publishers of third-party content), the claims are not barred by Section 230. Additionally, in one of the cases, a judge determined that the negligence cause of action was not barred by the First Amendment when the plaintiff's claims of harm were based on the design features of the platforms themselves, rather than specific online material.[200] These decisions simply concluded that Section 230 and the First Amendment do not provide social media companies with unprecedented blanket immunity from being held responsible for their own lack of ordinary care—just like every other business is responsible for ensuring their products are safe. Instead,

the courts found that whether such claims are barred will turn on the specific theories of liability and on a case-by-case basis: based on how the platforms actually operate as shown in discovery, rather than how they say they operate in court briefs.

Ultimately, with laws based on design features and decisions that platform companies made in rolling out their products, and in lawsuits brought by state attorneys general or private rights of action, liability will depend on whether the harms to children were caused by the social media companies' unilateral conduct (in which case the claims would not be barred), or third-party online material (in which case the claims may be barred). This will be left to the courts to decide, based on the discovery produced in the case and not the claims stated in legal briefs.

Product Liability Approach in the Context of Advanced Chatbots

Under traditional product liability rules, product manufacturers and sellers are responsible when their products injure consumers. Product manufacturers have a duty to produce safe products and can be responsible for manufacturing defects, design defects, and failure to warn consumers about risks. Historically, children's products have been held to higher safety standards.

Now that so many "products" are digital—including digital AI chatbots for children—there are multiple efforts to hold companies responsible for AI products as well. This played out in a recent AI chatbot case, *Garcia v. Character Technologies, Inc.*,[201] where it was argued that a Florida teenager took his own life after becoming emotionally dependent on the company's AI 'companion' features. [202] In that case, the court ruled that the plaintiff (the victim's mother) could pursue product claims, such as failure to warn, against the Character.AI app. The court also found that Google could be liable as a component part manufacturer because Google had supplied its cloud technical infrastructure to help power Character Technologies' LLM. In January of this year, Character.AI and Google settled this and several other cases out of court, in Colorado, New York, and Texas, for undisclosed amounts.[203] Several other wrongful death lawsuits have been filed against OpenAI in California state court. Recently a petition to coordinate 12 of these lawsuits was granted under JCCP 5431. As of February 2026 it had not been determined whether the trial judge will consolidate the cases for trial or if a bellwether (or representative) trial should occur. This is similar to what is occurring in Los Angeles Superior Court with the Social Media Addiction lawsuits mentioned previously.

Policy Recommendations

In 2025 alone, Common Sense Media supported legislation to increase the health and safety of kids online in eight states. Common Sense Media has significant experience working at the federal, state, and local levels, and maintains model legislative language that can be adapted to meet the needs of any state. While the interests and needs of individual lawmakers vary, the suite of policy solutions below can be the starting point for a larger conversation about child online safety, privacy, and overall well-being, and can build on the growing national momentum to put kids and families at the center of digital and AI policymaking. Voters across political parties overwhelmingly favor states taking action to protect their families. For 2026 and beyond, we recommend the following solutions.

- **Protect kids and teens from dangerous AI products**:[204] Codify baseline guardrails for all high-risk AI products, restrict unsafe features in AI chatbots used by kids, and promote safe and responsible technological innovation. Our research recommends against teens using AI chatbots for mental health or emotional support.[205]

- **Implement age assurance that protects privacy**: Require platforms that use harmful design features to determine users' ages with commercially reasonable and technically feasible tools that preserve user privacy, closing the loophole that lets companies claim ignorance of users' ages despite having vast amounts of data suggesting otherwise.
- **Protect young people's data:** Update outdated privacy protections to maintain efficacy in the AI era, limiting the collection, use, and sale of children's and teens' data, prohibiting targeted marketing to kids, and ensuring the most privacy-protective standards as the default for kids.
- **Hold social media companies accountable for their impacts on kids, and require them to improve their products**:[206] Hold social media companies responsible when their products cause harm to minors, and limit social media companies' ability to use addictive features, such as algorithmic feeds and push notifications, that keep kids glued to their devices. Two states have already enacted these limitations. Further, Congress should pass KOSA as it was introduced in the Senate in 2025 (S. 1748).
- **Empower families to make decisions about their social media use through social media warning labels**:[207] Require transparency about risks of harm to young users through warning labels on addictive social media platforms. Just as families deserve to know the risks of smoking and drinking, they should know that addictive social media feeds can take a toll on their kids' mental health and well-being. Four state legislatures have already signed various types of warning label bills into law.
- **Support digital and AI literacy and affordable broadband**: Ensure that all students are equipped with state-of-the-art digital and AI literacy instruction, and that they have access to the broadband service and devices they need to support meaningful use, at home and in school.
- **Ensure strong enforcement:** Whether in state or federal legislation, protecting children from online harms requires effective enforcement to hold companies accountable for legal obligations, including through well-funded expert regulators, private lawsuits, and attorneys general with the ability to impose fines and injunctions.

Conclusion

With a new sense of urgency propelled by the explosive growth of artificial intelligence, the landscape of children's online safety has fundamentally shifted. If 2025 was the year of *Free Speech Coalition, Inc. v. Paxton* and the year that AI companions revealed the glaring inadequacies of our online safety paradigm, then 2026 must be the year of structural accountability.

A critical part of this shift is legal. This report has detailed how the old tech industry playbook is showing signs of strain. The Supreme Court has opened a narrow but viable path for regulation, suggesting that laws focused on corporate conduct rather than speech may face only intermediate scrutiny. While not a panacea for every potential harm, this development suggests that a carefully executed move away from regulating content—and toward regulating business practices, such as design features—may bear significant fruit in the months ahead.

The most durable victories in kids' online safety will come from dismantling the specific features that are engineered to capture attention and keep kids glued to their screens. By targeting features like infinite scrolls, autoplay, and aggressive algorithmic recommendation, we can increase protections for children from manipulation without infringing on their rights to access information. But in lieu of these design changes, recent court decisions have left the door open for social media delays or bans as an option to keep kids safe in these online spaces.

As we move forward to address many of the harms that proliferated during the past two decades of unregulated social media, we must be vigilant in handling the rapidly evolving frontier of AI programs, including AI companions specifically. We cannot wait another 20 years to address these harms, because these technologies are already exploiting vulnerabilities in our legal system and in our children's psychology. We must adopt pre-market safety assessments and robust age-gating for high-risk AI products before this technology becomes entrenched.

Yet safety laws and litigation together will still prove insufficient to the task of keeping our kids safe online if the digital playing field remains uneven. As we push for tighter regulations, we must also close the persistent digital divide that leaves millions of families behind. True digital well-being requires that all children and their families have access to high-quality, affordable broadband and the literacy skills to carefully use the internet. This will ensure that the benefits of the digital and AI economy are distributed across society, not reserved just for the privileged few.

The momentum is now firmly on the side of parents and other advocates and their allies in legislatures and courtrooms across the country and globally working to safeguard the well-being of kids and families. The laissez-faire approach to kids' online safety is being tested, and these challenges will open the door to a safer and healthier future for our kids in a new digital age.

Endnotes

1. Alter, C. (2025). Court filings allege Meta downplayed risks to children and misled the public. *Time*. https://time.com/7336204/meta-lawsuit-files-child-safety/.
2. Radesky, J., Weeks, H. M., et al. (2023). *Constant companion: A week in the life of a young person's smartphone use.* Common Sense Media. https://www.commonsensemedia.org/sites/default/files/research/report/2023-cs-smartphone-research-report_final-for-web.pdf.
3. Mann, S., Robb, M. B., & Fox Johnson, A. (2026). *Age assurance attitudes among adults*. Common Sense Media. https://www.commonsensemedia.org/research/age-assurance-attitudes-among-adults.
4. Online Safety Law Center. *U.S. online safety law tracker*. https://onlinesafety.orrick.com/.
5. *Computer & Communications Industry Association v. Paxton*, No. 1:24-cv-00849 (W.D. Tex. 2024). https://storage.courtlistener.com/recap/gov.uscourts.txwd.1172798016/gov.uscourts.txwd.1172798016.1.0.pdf.
6. Ferguson, H., Brundson, V., & Bradford, E. (2021). The developmental trajectories of executive function from adolescence to old age. *Scientific Reports*. https://doi.org/10.1038/s41598-020-80866-1.
7. Sun, K, Sugatan, C., et al. (2021). "They see you're a girl if you pick a pink robot with a skirt": how children conceptualize data processing and digital privacy risks. *CHI '21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. https://dl.acm.org/doi/10.1145/3411764.3445333.
8. Crone, E. (2009). Executive functions in adolescence: inferences from brain and behavior. *Developmental Science*. https://doi.org/10.1111/j.1467-7687.2009.00918.x; Galvan, A. (2010). Adolescent development of the reward system. *Frontiers in Human Neuroscience*, 4, 6. https://doi.org/10.3389/neuro.09.006.2010.
9. Parr, A. C., Calabro, F., et al. (2021). Dopamine-related striatal neurophysiology is associated with specialization of frontostriatal reward circuitry through adolescence. *Progress in Neurobiology*, 201, 101997.
10. Abrams, Z. (2022). *Why young brains are especially vulnerable to social media*. APA. https://www.apa.org/news/apa/2022/social-media-children-teens.
11. Wilcox, B. L., et al. (2004). *Report of the APA task force on advertising and children*. APA. https://www.apa.org/pubs/reports/advertising-children.
12. Joseff, K. (2022). *Behavioral advertising harms: kids and teens*. Common Sense Media. https://www.commonsensemedia.org/sites/default/files/featured-content/files/behavioral_-surveillance-advertising-brief.pdf.
13. Ibid.
14. Solove, D. (2024). Artificial intelligence and privacy. *Florida Law Review* 77(1). http://dx.doi.org/10.2139/ssrn.4713111.
15. Guo, E. (2025). A major AI training data set contains millions of examples of personal data. *Technology Review*. https://www.technologyreview.com/2025/07/18/1120466/a-major-ai-training-data-set-contains-millions-of-examples-of-personal-data/.
16. Ahmed, A., Feder Cooper, A., et al. (2026). *Extracting books from production language models*. (arXiv No. 2601.02671). arXiv. https://doi.org/10.48550/arXiv.2601.02671.
17. Gellman, R. (2025). Is there any way forward for privacy legislation in the United States? *Tech Policy Press*. https://www.techpolicy.press/is-there-any-way-forward-for-privacy-legislation-in-the-united-states/.
18. SuperAwesome. (2018). *SuperAwesome launches kid-safe filter to prevent online ads from stealing children's personal data*. https://www.superawesome.com/superawesome-launches-kid-safe-filter-to-prevent-online-ads-from-stealing-childrens-personal-data/.
19. U.S. Department of Health and Human Services. (2023). *Social media and youth mental health: The U.S. surgeon general's advisory* (PDF). https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf.
20. Radesky et al., *A week in the life of a young person's smartphone use.*
21. Alter. *Court filings allege Meta downplayed risks to children and misled the public.*
22. Haugen, F. (2021). Written testimony before the Subcommittee on Consumer Protection, Product Safety, and Data Security, United States Senate Committee on Commerce, Science, and Transportation. https://www.commerce.senate.gov/services/files/FC8A558E-824E-4914-BEDB-3A7B1190BD49.
23. *Hidden harms: examining whistleblower allegations that Meta buried child safety research, hearing before the Subcommittee on Privacy, Technology, and the Law of the United States Senate Committee on the Judiciary.* (2025). https://www.judiciary.senate.gov/committee-activity/hearings/hidden-harms-examining-whistleblower-allegations-that-meta-buried-child-safety-research. Haugen, ibid.

24. Chen, M. L. (2023). *How screen time is affecting teens' sleep and mental health*. World Economic Forum. https://www.weforum.org/stories/2023/09/screen-time-affecting-sleep-mental-health/.
25. Common Sense Media. (2025). Research brief: *Teens, trust, and technology in the age of AI*. https://www.commonsensemedia.org/research/research-brief-teens-trust-and-technology-in-the-age-of-ai.
26. Issue One. (2024). *New poll finds near universal public support for bipartisan legislation protecting kids online.* https://issueone.org/press/new-poll-finds-near-universal-public-support-for-bipartisan-legislation-protecting-kids-online/.
27. Kids Code Coalition. (n.d.). https://kidscodecoalition.org.
28. Children and Screens. (2024). *UK's Age Appropriate Design Code ushers in nearly 100 safe digital space changes for youth.* https://www.childrenandscreens.org/newsroom/news/uks-age-appropriate-design-code-ushers-in-nearly-100- safe-digital-space-changes-for-youth/.
29. The CA AADC had an original effective date of July 1, 2024.
30. *NetChoice v. Bonta*, No. 23-CV-12345 (N.D. Cal. Apr. 11, 2025). Notice of Appeal. https://oag.ca.gov/system/files/attachments/press-docs/%5B146%5D%20NetChoice%20v.%20Bonta%20-%20Notice%20of%20Appeal%204.11.2025.pdf.
31. This case is pending under case number 1:25-cv-00322-RDB in the District Court of Maryland.
32. New York State Governor's Office. (2026). *Protecting our kids: Governor Hochul announces nation-leading proposals to protect kids online, restrict AI chatbots and combat the youth mental health crisis*. https://www.governor.ny.gov/news/protecting-our-kids-governor-hochul-announces-nation-leading-proposals-protect-kids-online.
33. Gounardes, A., & Steyer, J. (2025). Commentary: We need to talk about the Roblox problem. *Times Union*. https://www.timesunion.com/opinion/article/commentary-need-talk-roblox-problem-21223657.php.
34. Kleinman, Z., & Hayes, G. (2025). Keep kids off Roblox if you're worried, its CEO tells parents. *BBC*. https://www.bbc.com/news/articles/c5yrjkl7dd6o.
35. Carville, O., & D'Anastasio, C. (2024). Roblox's pedophile problem. *Bloomberg*. https://www.bloomberg.com/features/2024-roblox-pedophile-problem/.
36. Albarado, S. (2025). Federal judge declares Arkansas social media age-verification law unconstitutional. *Arkansas Advocate*. https://arkansasadvocate.com/2025/04/01/federal-judge-declares-arkansas-social-media-age-verification-law-unconstitutional/.
37. Odzer, A. (2025). *Florida law banning kids from social media takes effect after court rules in favor*. NBC6 South Florida. https://www.nbcmiami.com/news/local/florida-social-media-ban-teens-kids-law/3729138/.
38. Williams, R. (2025). Judge blocks Georgia's new social media age verification law just before it was set to start. *Georgia Recorder*. https://georgiarecorder.com/briefs/judge-blocks-georgias-new-social-media-age-verification-law-just-before-it-was-set-to-start/.
39. LaRose, G. (2025). Louisiana's age-check law for social media is unconstitutional, federal judge rules. *Louisiana Illuminator*. https://lailluminator.com/2025/12/18/louisiana-social-media-2/.
40. *Miss. H.B. 1126* ("Walker Montgomery Protecting Children Online Act"), 2024 Reg. Sess. (Miss. 2024), https://billstatus.ls.state.ms.us/documents/2024/html/HB/1100-1199/HB1126PS.htm.
41. Evans, N. (2025). Ohio judge permanently blocks social media age verification law. *Ohio Capital Journal*. https://ohiocapitaljournal.com/2025/04/18/ohio-judge-permanently-blocks-social-media-age-verification-law/.
42. PRIVO. (2025). *What is the Tennessee 'Protecting Children from Social Media Act' and how to comply*. https://www.privo.com/blog/tennessee-protecting-children-from-social-media-act-1.
43. Supreme Court of the United States. (2025). *NetChoice, LLC v. Lynn Fitch*, No. 25A97. https://www.supremecourt.gov/opinions/24pdf/25a97_5h25.pdf.
44. Matat, S. (2025). Florida has green light to restrict minors' social media access. *Tallahassee Democrat*. https://www.tallahassee.com/story/news/local/state/2025/11/25/florida-can-enforce-law-restricting-minors-social-media-access/87470906007/.
45. Dr. Murthy was appointed to the Board of Common Sense Media in fall 2025.
46. Murthy, V. (2024). Surgeon general: Why I'm calling for a warning label on social media platforms. *New York Times*. https://www.nytimes.com/2024/06/17/opinion/social-media-health-warning.html.
47. Lima-Strong, C. (2024). 42 state AGs endorse federal plan to add warning labels on social media. *Washington Post*. https://www.washingtonpost.com/technology/2024/09/10/state-attorneys-endorse-social-media-warning-labels.
48. United States Congress. (2025). *Stop the Scroll Act* (S. 1885). https://www.congress.gov/bill/119th-congress/senate-bill/1885.

49. California Legislature. Assembly Bill 2: *Injuries to children: civil penalties* (AB 2). https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260AB2 and (2024) https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB3172.
50. Institute of Education Sciences. (2025). *More than half of public school leaders say cell phones hurt academic performance*. U.S. Department of Education.
51. Haidt, J. (2024). *The anxious generation: How the great rewiring of childhood is causing an epidemic of mental illness.* Penguin Press.
52. Common Sense Media. (2025). Comments to the Australian e-safety commissioner on *Designing for safety: Preventing grievous harm before it happens* draft report. https://www.commonsensemedia.org/sites/default/files/featured-content/files/aus-e-safety-comments-common-sense-media-october-2025.pdf.
53. Common Sense Media. (2025). Comments to the European Commission on the *DSA - Digital Fairness Act* call for evidence. https://www.commonsensemedia.org/sites/default/files/featured-content/files/common-sense-media-comments-dsa-digital-fairness-act-call-for-evidence.pdf.
54. DSA Comments on Protection of Minors Guidance (2025).
55. Ofcom Comments on A Safer Life Online for Women and Girls Consultation (2025).
56. Ofcom Comments on Illegal Harms: User Controls Consultation (2025).
57. Ofcom Comments on Online Safety: Additional Safety Measures (2025).
58. Ofcom Comments on Call for Evidence: Statutory Reports on Age Assurance & App Stores (2025).
59. Cerulus, L. (2025). Vance's week of waging war on EU tech law. *Politico*. https://www.politico.eu/article/jd-vance-waging-war-eu-tech-law-msc-ai-summit/.
60. O'Carroll, L. (2025). Elon Musk's X fined €120m by EU in first clash under new digital laws. *The Guardian*. https://www.theguardian.com/technology/2025/dec/05/elon-musk-x-fined-eu-first-clash-under-new-digital-laws.
61. Australian Government, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts. (2025). *Social media minimum age*. https://www.infrastructure.gov.au/media-communications/internet/online-safety/social-media-minimum-age.
62. Ibid.
63. Kaye, B. (2025). Australian leader defends social media ban as teens flaunt workarounds. *Reuters*. https://www.reuters.com/business/media-telecom/australia-leader-defends-social-media-ban-teens-brag-about-staying-online-2025-12-11/.
64. Pesheva, E. (2024). Using AI to repurpose existing drugs for treatment of rare diseases. *Harvard Gazette*. https://news.harvard.edu/gazette/story/2024/09/using-ai-to-repurpose-existing-drugs-for-treatment-of-rare-diseases/.
65. *Is AI making the workforce more productive?* (2024). Bipartisan Policy Center. https://bipartisanpolicy.org/article/is-ai-making-the-workforce-more-productive/.
66. Chow, A. (2025). ChatGPT may be eroding critical thinking skills, according to a new MIT study. *Time*. https://time.com/7295195/ai-chatgpt-google-learning-school/.
67. National Conference of State Legislatures. (2025). Artificial intelligence 2025 legislation. https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation.
68. Samuel, S. (2024). People are falling in love with—and getting addicted to—AI voices. *Vox*. https://www.vox.com/future-perfect/367188/love-addicted-ai-voice-human-gpt4-emotion?utm_source=chatgpt.com.
69. Hao, K. (2025). *Empire of AI*. Penguin Press.
70. Verma, P., Tiku, N., & Zakrzewski, C. (2024). OpenAI promised to make its AI safe. Employees say it 'failed' its first test. *Washington Post*. https://www.washingtonpost.com/technology/2024/07/12/openai-ai-safety-regulation-gpt4/.
71. Hendrix, J. (2025). US Senate drops proposed moratorium on state AI laws in budget vote. *Tech Policy Press*. https://www.techpolicy.press/us-senate-drops-proposed-moratorium-on-state-ai-laws-in-budget-vote/.
72. The White House. (2025). *Ensuring a national policy framework for artificial intelligence*. https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/.
73. Kang, C. (2025). Trump signs executive order to neuter state A.I. laws. *New York Times*. https://www.nytimes.com/2025/12/11/technology/ai-trump-executive-order.html.

74. McGrail, B. (2026). The AI preemption executive order's BEAD strategy faces steep legal hurdles. *Lawfare*. https://www.lawfaremedia.org/article/the-ai-preemption-executive-order-s-bead-strategy-faces-steep-legal-hurdles.
75. The White House. (2025). *Advancing artificial intelligence education for American youth*. https://www.whitehouse.gov/presidential-actions/2025/04/advancing-artificial-intelligence-education-for-american-youth/.
76. U.S. Senator Amy Klobuchar. (2025). *Klobuchar's bipartisan TAKE IT DOWN Act signed into law*. https://www.klobuchar.senate.gov/public/index.cfm/2025/5/klobuchar-s-bipartisan-take-it-down-act-signed-into-law.
77. Common Sense Media. *AI risk assessments*. (n.d.). https://www.commonsensemedia.org/ai-ratings/ai-risk-assessments. Common Sense Media. *AI risk assessments*. (n.d.). https://www.commonsensemedia.org/ai-ratings/ai-risk-assessments.
78. Hill, K. (2025). A teen was suicidal. ChatGPT was the friend he confided in. *New York Times*. https://www.nytimes.com/2025/08/26/technology/chatgpt-openai-suicide.html.
79. Roose, K. (2025). Can A.I. be blamed for a teen's suicide? *New York Times*. https://www.nytimes.com/2024/10/23/technology/characterai-lawsuit-teen-suicide.html.
80. Horwitz, J. (2025). Meta's flirty AI chatbot invited a retiree to New York. He never made it home. *Reuters*. https://www.reuters.com/investigates/special-report/meta-ai-chatbot-death/.
81. Raine v. OpenAI complaint. (2025). *DocumentCloud*. https://www.documentcloud.org/documents/26078522-raine-vs-openai-complaint/Raine v. OpenAI.
82. Montoya v. Character Technologies, Inc.
83. Reiley, L. (2025). What my daughter told ChatGPT before she took her life. *New York Times*. https://www.nytimes.com/2025/08/18/opinion/chat-gpt-mental-health-suicide.html.
84. Betts, A. (2025). ChatGPT accused of acting as "suicide coach" in series of US lawsuits. *The Guardian*. https://www.theguardian.com/technology/2025/nov/07/chatgpt-lawsuit-suicide-coach.
85. Black, L., & Council, S. (2026). A Calif. teen trusted ChatGPT for drug advice. He died from an overdose. *SFGate*. https://www.sfgate.com/tech/article/calif-teen-chatgpt-drug-advice-fatal-overdose-21266718.php.
86. Dupré, M. H. (2026). ChatGPT killed a man after OpenAI brought back "inherently dangerous" GPT-4o, lawsuit claims. *Futurism*. https://futurism.com/artificial-intelligence/chatgpt-suicide-openai-gpt4o.
87. Common Sense Media. (2025). *AI companions decoded: Common Sense Media recommends AI companion safety standards*. https://www.commonsensemedia.org/press-releases/ai-companions-decoded-common-sense-media-recommends-ai-companion-safety-standards.
88. Coalition letter to the U.S. Department of Education re: AI in education. (2025). *DocumentCloud*. https://www.commonsensemedia.org/sites/default/files/featured-content/files/coalition-letter-to-u.s-doe-re-ai-in-education.pdf.
89. Common Sense Media. (2026). *AI toys*. https://www.commonsensemedia.org/ai-ratings/ai-toys.
90. DiPaola, D., & Calo, R. (2024). *Socio-digital vulnerability* (SSRN Scholarly Paper No. 4686874). SSRN. https://doi.org/10.2139/ssrn.4686874.
91. Girouard-Hallam, 2021, 2022, and 2023.
92. DiPaola & Calo. *Socio-digital vulnerability*.
93. Bender, E., Gebru, T., et al. (2021). On the dangers of stochastic parrots: Can language models be too big? In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*. Association for Computing Machinery. https://dl.acm.org/doi/10.1145/3442188.3445922.
94. Common Sense Media. (2024). *The dawn of the AI era: Teens, parents, and the adoption of generative AI at home and school*. https://www.commonsensemedia.org/research/the-dawn-of-the-ai-era-teens-parents-and-the-adoption-of-generative-ai-at-home-and-school.
95. Common Sense Media. (2025). *Talk, trust, and trade-offs: how and why teens use AI companions*. https://www.commonsensemedia.org/research/talk-trust-and-trade-offs-how-and-why-teens-use-ai-companions.
96. Common Sense Media. (2025). *Teens, trust, and technology in the age of AI*. https://www.commonsensemedia.org/research/research-brief-teens-trust-and-technology-in-the-age-of-ai.
97. Common Sense Media. (2025). *Model state legislation on AI companions & justification for AI safeguards for kids*. https://www.commonsensemedia.org/sites/default/files/featured-content/files/model-state-legislation-justification-for-ai-safeguards-for-kids.pdf.

98. *Human-like AI legislative framework*. Young People's Alliance https://smggrfyky6jfw5l3.public.blob.vercel-storage.com/humanlike-ai.pdf.
99. Winters, B., Williams, K. & Bouffard, B. (2026). Model legislation: People-first chatbot bill. *Fair Play for Kids.* https://fairplayforkids.org/wp-content/uploads/2026/01/People-First-Chatbot-Bill-Jan-20-2026-1.pdf.
100. *Safeguarding Adolescents From Exploitative Chatbots and Humanlike AI Technologies, Ethics and Public Policy Center.* https://eppc.org/wp-content/uploads/2025/10/The-SAFE-CHAT-Act.pdf
101. Shapero, J. (2025). Parents call for guardrails on AI chatbots after suicides, self-harm. *The Hill.* https://thehill.com/policy/technology/5506813-parents-testify-ai-chatbots-suicide/.
102. Toscano, M., & Burchfiel, K. (2025). *Americans want A.I. safeguards by a 9-to-1 margin*. Institute for Family Studies. https://ifstudies.org/blog/americans-want-ai-safeguards-by-a-9-to-1-margin.
103. Jenkins, A. (2025). *AGs warn AI companies on kid safety*. Pluribus News. https://pluribusnews.com/news-and-events/ags-warn-ai-companies-on-kid-safety/.
104. Gluck, J. (2025). *Understanding the new wave of chatbot legislation: California SB 243 and beyond*. Future of Privacy Forum. https://fpf.org/blog/understanding-the-new-wave-of-chatbot-legislation-california-sb-243-and-beyond/.
105. VA HB635. https://lis.virginia.gov/bill-details/20261/HB635.
106. MI S760. https://legislature.mi.gov/documents/2025-2026/billintroduced/Senate/pdf/2025-SIB-0760.pdf.
107. NY S9051, https://legislation.nysenate.gov/pdf/bills/2025/S9051.
108. Children's Personal Photos Are Powering AI Exploitation, *Human Rights Watch.*
109. How Photos of Your Kids Are Powering Surveillance Technology, *New York Times.*
110. Investigation Finds AI Image Generation Models Trained on Child Abuse, Stanford Cyber Policy Center.
111. https://www.commonsensemedia.org/sites/default/files/featured-content/files/common-sense-media-feedback-on-the-eu-ai-act-and-high-risk-ai.pdf.
112. https://www.politico.com/news/2025/09/29/newsom-signs-ai-law-00585348.
113. https://www.governor.ny.gov/news/governor-hochul-signs-nation-leading-legislation-require-ai-frameworks-ai-frontier-models.
114. UNESCO on AI; Information Week on AI.
115. Tinubu Ali, T., et al. Looking back, looking forward: What it will take to permanently close the K–12 digital divide (Jenny Pritchett ed. 2021). Common Sense Media. https://www.commonsensemedia.org/sites/default/files/featured-content/files/final_-_what_it_will_take_to_permanently_close_the_k-12_digital_divide_vfeb3.pdf.
116. Cameron Marx. (2025). *NTIA approves updated BEAD initial proposals from all 56 states and territories*. Broadband Breakfast. https://broadbandbreakfast.com/ntia-approves-updated-bead-initial-proposals-from-all-56-states-and-territories/.
117. Executive Order, The White House, December 11, 2025, https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/.
118. Leasor, B. (2025). *New York's broadband law sets a new benchmark for access*. Tech Policy Press. https://www.techpolicy.press/new-yorks-broadband-law-sets-a-new-benchmark-for-access/.
119. Arnold, J. (2025). *Achieving Affordability: State Strategies for Getting Everyone Online.* Benton Institute for Broadband and Society. https://www.benton.org/blog/how-states-are-making-broadband-more-affordable
120. Gonsalves, S. (2026). *With ACP Gone, New Mexico Creates First State-Level Internet Affordability Program.* Community Networks. https://communitynetworks.org/content/acp-gone-new-mexico-creates-first-state-level-internet-affordability-program.
121. Hutton, Z. (2023). States begin to address media literacy through legislation. Governing. https://www.governing.com/education/states-begin-to-address-media-literacy-through-legislation.
122. Media Literacy Now. *Putting media literacy on the public policy agenda.* https://medialiteracynow.org/impact/current-policy/.
123. *See e.g.*, Arizona Standards; Iowa Standards.
124. North Carolina H 959. https://legiscan.com/NC/bill/H959/2025.
125. AI for education. *State AI guidance for K12 schools*. https://www.aiforeducation.io/ai-resources/state-ai-guidance.
126. Dwyer, M. (2025). *Looking back at AI guidance across state education agencies and looking forward*. Center for Democracy & Technology. https://cdt.org/insights/looking-back-at-ai-guidance-across-state-education-agencies-and-looking-forward/.
127. California ABA 2876 ; Connecticut HB 5524 (Sections 143-144); Indiana Department AI Tutor Pilot Program; Iowa Department AI Tutor Program.

128. Common Sense Media. *Digital citizenship curriculum*. https://www.commonsense.org/education/digital-citizenship.
129. Techtarget Article on Major Tech Cases; Dynamis LLP article on Section 230.
130. Under preexisting laws, attorneys general are bringing lawsuits under consumer protection and deceptive trade practices laws. They claim that tech companies deceived consumers on their data privacy protections, the addictive quality of their platforms, and the age appropriateness of their platforms. *See e.g.*, Rokita v. Google (claiming deceptive trade practices regarding collection and usage of consumer data); In re: Social Media Addiction/Personal Injury Products Liability Litigation (claiming deceptive trade practices for the harmful effects of social media and claiming a failure to comply with federal law on data privacy); and Coleman v. Kentucky (claiming deceptive trade practices for presenting social media as safe for children). New laws, such as those requiring age verification or protecting consumer data, provide claims focused squarely on the tech industry. *See e.g.*, Uthmeier v. Snap (suing for failure to comply with HB 3 which requires age verification for social media platforms); and Brown v. Snap (suing for violations of the Utah Consumer Privacy Act which requires reasonably accessible and clear privacy notice for data practices).
131. Attorney general-led lawsuits utilizing new laws or provisions include Texas, Arkansas, and Connecticut, with Texas's SCOPE Act acting as a strong source for claims. Texas v. TikTok (SCOPE); Texas Inquiries (SCOPE); Arkansas v. Temu (Arkansas Personal Information Act); Connecticut Fine (Connecticut Data Privacy Act). Illinois consumers can utilize a strong private right of action in the Illinois Biometric Information Privacy Act ("BIPA"), while other consumers must use general negligence or trade practices laws. *See e.g.*, Rivera v. Google (suing under BIPA and settling for $100 million); In re Clearview AI , Inc., Consumer Privacy Litigation (suing under BIPA and general Virginia, New York, and California state laws before settling for $51.75 million).
132. Netchoice litigates many lawsuits against internet regulation, and its association members include the internet's top brands, including all major social media companies. See NetChoice About Us and NetChoice v. Bonta Complaint (CAADCA case).
133. NetChoice v. Bonta Preliminary Injunction (CAADCA case); NetChoice v. Skrmetti Preliminary Injunction (Parental Consent on Social Media).
134. TikTok v. Garland; NetChoice lawsuit against CFPB; Google's lawsuit against CFPB; Public Interest Privacy Center Tracker (22 lawsuits against child privacy laws according to the tracker).
135. Netchoice v. Griffin (age verification and addictive design); Computers and Communication Industry Association v. Uthmeier (age-gating social media); NetChoice v. Bonta (data privacy and harmful design features); Netchoice v. Finch (content moderation obligations).
136. Netchoice v. Griffin at 43-44, 52 (new law); Netchoice v. Bonta at 27 (CAADCA); Netchoice v. Finch at 34-36; Computers and Communications Industry v. Paxton at 34-35; Netchoice v. Reyes at 39-41, 43, 52.
137. Computers and Communications Industry v. Uthmeier at 27-33; Netchoice v. Griffin at 22-24 (old, stricken law); Netchoice v. Carr at 30-34; Netchoice v. Murrill at 21-25; Netchoice v. Yost at 20-25; NetChoice v. Skrmetti at 18-21.
138. Snap v. Brown at 23-24.
139. Garcia v. Character Technologies at 31-33.
140. Computers and Communications Industry v. Uthmeier at 32; Netchoice v. Griffin at 31-35, 44-46 (new law); Snap v. Brown at 21-24); Netchoice v. Bonta at 19-21 (CAADCA); Netchoice v. Bonta at 19-22 (addiction act); Netchoice v. Finch at 19-20; Computers and Communications Industry v. Paxton at 21-25, 26-32; Netchoice v. Reyes at 27-30, 34-39.
141. Computers and Communications Industry v. Uthmeier at 40-43; Netchoice v. Griffin at 40-43 (new law); Netchoice v. Bonta at 22-24 (CAADCA); Netchoice v. Bonta at 25-26 (addiction act); Netchoice v. Carr at 38-40; Netchoice v. Murrill at 28-29; Netchoice v. Finch at 23-24, 33-34; Netchoice v. Yost at 29-32; NetChoice v. Skrmetti at 23-25; Computers and Communications Industry v. Paxton at 25-26, 32-34; Netchoice v. Reyes at 32-34.
142. Snap v. Brown and Netchoice v. Bonta (addiction act) dealt with the right to peaceful assembly. Computers and Communications Industry v. Uthmeier and Netchoice v. Bonta (CAADCA) dealt with COPPA.
143. Netchoice v. Carr at 48-50; Netchoice v. Murrill at 35-36.
144. Netchoice v. Carr at 30, 34; Netchoice v. Bonta at 20, 22 (addiction act); Netchoice v. Murrill at 21, 25; Netchoice v. Finch at 19, 21; Netchoice v. Yost at 20, 25; NetChoice v. Skrmetti at 18, 21; Netchoice v. Reyes at 27, 30.
145. *See e.g.*, Netchoice v. Carr; Netchoice v. Bonta (addiction act); Netchoice v. Murrill.
146. Netchoice v. Griffin at 33-34 (old, stricken law); Lawfare Article.
147. Katzenberger, T. (20250. *Google, Meta, TikTok sue California over 'addictive' social media feeds law*. PoliticoPro. https://subscriber.politicopro.com/article/2025/11/google-youtube-sue-california-over-addictive-social-media-feeds-law-00652353.

148. *See e.g.*, Wayne Jones v. Mean LLC (Complaint) (individual lawsuit for design of multiple social media platforms helped to radicalize a mass shooter, leading to death of victim represented by plaintiff); In Re: Social Media Adolescent Addiction (Motion to Transfer)(class action for product liability and other claims regarding the impact of Facebook's and Instagram's designs upon adolescents).
149. Kang, C. (2026). Social media giants face landmark legal tests on child safety. *New York Times.* https://www.nytimes.com/2026/01/27/technology/social-media-addiction-trial.html.
150. Social Media Cases, Judicial Council Coordination Case No. JCCP 5255 (Los Angeles Superior Court), October 2023.
151. Neville v. Snap; Lemmon v. Snap; Anderson v. TikTok; Wozniak v. YouTube; State of N.C. v. TikTok Inc.
152. Section 230.
153. Lemmon v. Snap at 13-14,17.
154. Anderson v. TikTok at 10-11.
155. Wozniak v. YouTube at 33-34.
156. Lemmon v. Snap at 13-14,17; Anderson v. TikTok at 10-11; Wozniak v. YouTube at 33.
157. https://time.com/7336204/meta-lawsuit-files-child-safety/.
158. A.F., on behalf of J.F. v. Character Technologies, Inc. (Complaint)(Order to Compel); *see e.g.*, Flora v. Prism Labs, Inc. (Complaint)(Compel Arbitration)(class action lawsuit on data privacy).
159. P.M. v. OpenAI LP (Complaint) (Dismissal); *see e.g.*, T. v. OpenAI LP (Order)(case closed after plaintiff chose to not amend complaint).
160. Katz-Lacabe v. Oracle America, Inc. (Complaint) (Approval of Settlement).
161. In Re: Clearview AI, Inc., Consumer Privacy Litigation (Memorandum Opinion).
162. Alter, C. (2026). Court filings allege Meta downplayed risks to children and misled the public. *New York Times.* https://www.nytimes.com/2026/01/20/technology/snap-social-media-addiction-lawsuit.html; and Duffy, C. (2026). Meta and YouTube head to trial to defend against youth addiction, mental health harm claims. *CNN.*
163. Another way that tech companies can avoid publicity is through intellectual property law. Software can contain trade secrets and prevent examination of their algorithmic code for issues. *See e.g.*, Rayner v. New York State Department of Corrections at *6-7 (finding that the code and documents detailing an algorithm's formulas could not be disclosed in a Freedom of Information claim, as this information was a trade secret).
164. Noyb. (2025). *Bumble's AI icebreakers are mainly breaking EU law.* https://noyb.eu/en/bumbles-ai-icebreakers-are-mainly-breaking-eu-law.
165. Australia eSafety media release.
166. Savarese, M., & Hughes, E. (2025). Brazil's Supreme Court justices agree to make social media companies liable for user content. *AP.* https://apnews.com/article/brazil-social-media-supreme-court-user-content-33312c07ddfae598f4d673d1141d6a4f.
167. Scott + Scott. Dutch court hands down ruling in case against TikTok. https://scott-scott.com/dutch-court-hands-down-ruling-in-case-against-tiktok/.
168. Netchoice v. Fitch at 14 (Appellate Opinion); Netchoice v. Skrmetti at 17-18, 22-23, 26 (Denied Preliminary Injunction).
169. Losey. *Federal appeals court allows Florida to enforce social media law regulating social media use by minors.* https://www.losey.law/federal-appeals-court-allows-florida-to-enforce-social-media-law-regulating-social-media-use-by-minors/.
170. National Conference of State Legislatures. (2025). *Social media and children 2025 legislation.* https://www.ncsl.org/technology-and-communication/social-media-and-children-2025-legislation.
171. Free Speech Coalition v. Paxton.
172. CCIA v. Paxton (W.D. Tex. 2025) (Dec 23 Order).
173. Free Speech Coalition v. Paxton citing Ginsberg v. New York, 390 U.S. 629 (1968).
174. Reno v. ACLU, 521 U.S. 844 (1997).
175. Ashcroft v. ACLU, 542 U.S. 656 (2004).
176. CCIA v. Paxton (W.D. Tex. 2025) (Dec 23 Order).
177. Free Speech Coalition v. Paxton.
178. Moody v. Netchoice, LLC, 603 U.S. 707, 724-26 (2024).
179. Moody v. Netchoice, LLC, 603 U.S. 707, 713, 724-26 (2024). A facial challenge is when a law is challenged as unconstitutional before it is effective. Moody v. Netchoice, LLC, 603 U.S. 707, 723 (2024).
180. Moody v. Netchoice, LLC, 603 U.S. 707, 731-32, 744 (2024).
181. Moody v. Netchoice, LLC, 603 U.S. 707, 734 (2024).

182. Moody v. Netchoice, LLC, 603 U.S. 707, 737-38, 740-743 (2024).
183. *See e.g.*, NetChoice v. Bonta at 18-21 (filed before *Moody*); NetChoice v. Finch at 18-22 (filed before *Moody*); Netchoice v. Murrill at 20-27 (filed after *Moody*); NetChoice v. Griffin at 30-40 (filed after *Moody*).
184. *See e.g.*, NetChoice v. Bonta at 19-20 (filed before *Moody*); NetChoice v. Finch at 19-20 (filed before *Moody*); NetChoice v. Murrill at 21-25 (filed after *Moody*); NetChoice v. Griffin at 33-35 (filed after *Moody*); Netchoice Letter.
185. NetChoice v. Bonta, U.S. District Court for the Northern District of California (2024).
186. Anderson v. TikTok. While the Supreme Court touched upon the issue, it never gave a definitive statement on whether algorithms had First Amendment protection, and instead focused on the method of analysis for facial challenges. Moody v. NetChoice.
187. Anderson v. TikTok.
188. Congressional Report on Section 230.
189. Durbin press release.
190. KOSA bill.
191. Crowell Article. Agencies like the FCC have shown interest in their rule-making authority regarding Section 230 since 2020. FCC's Section 230 Rulemaking.
192. Lemmon v. Snap; Anderson v. TikTok; Wozniak v. YouTube.
193. Rocha, N. (2026). Google and Character.AI to settle lawsuit over teenager's death. *New York Times*. https://www.nytimes.com/2026/01/07/technology/google-characterai-teenager-lawsuit.html.
194. Tiku, N., & Sands, L. (2025). Judge rejects claim chatbots have free speech in suit over teen's death. *Washington Post*. https://www.washingtonpost.com/nation/2025/05/22/sewell-setzer-suicide-ai-character-court-lawsuit/.
195. Fox Johnson, A. (2025). *From dolls to downloads: Courts reimagine product liability for the digital age*. Tech Policy Press. https://www.techpolicy.press/from-dolls-to-downloads-courts-reimagine-product-liability-for-the-digital-age/.
196. Common Sense Media. (2025). *Social AI companions risk assessment*. https://www.commonsensemedia.org/sites/default/files/pug/csm-ai-risk-assessment-social-ai-companions_final.pdf.
197. EU AI Act.
198. California AB-2: Injuries to children: civil penalties. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260AB2.
199. Social Media Cases, Judicial Council Coordination Case No. JCCP 5255 (Los Angeles Superior Court), October 2023; and Neville v. Snap, Inc., Case No. 22STCV33500 (Los Angeles Superior Court), January 2024.
200. Ibid.
201. Tech Policy Press. *Tracker detail: Megan Garcia v. Character Technologies, Et Al*. https://www.techpolicy.press/tracker/megan-garcia-v-character-technologies-et-al/.
202. https://storage.courtlistener.com/recap/gov.uscourts.flmd.433581/gov.uscourts.flmd.433581.115.0.pdf.
203. Duffy, C. (2026). Character.AI and Google agree to settle lawsuits over teen mental health harms and suicides. *CNN*. https://www.cnn.com/2026/01/07/business/character-ai-google-settle-teen-suicide-lawsuit.
204. Common Sense Media. Model state legislation on AI companions and justification for AI safeguards for Kids. https://www.commonsensemedia.org/sites/default/files/featured-content/files/model-state-legislation-justification-for-ai-safeguards-for-kids.pdf.
205. Common Sense Media. (2025). *Social AI companions risk assessment*. https://www.commonsensemedia.org/sites/default/files/pug/csm-ai-risk-assessment-social-ai-companions_final.pdf.
206. Common Sense Media. *Model state legislation and justification for protections on addictive social media design*. https://www.commonsensemedia.org/sites/default/files/featured-content/files/model-state-legislation-justification-for-an-addictive-features-bill.pdf.
207. Common Sense Media. *Model state legislation on social media warning labels and justification for protecting kids online.* https://www.commonsensemedia.org/sites/default/files/featured-content/files/model-state-legislation-justification-for-social-media-warning-labels.pdf.

www.commonsense.org