North Dakota Legislative Council

Prepared for the Artificial Intelligence
and Data Center Committee
LC# 27.9243.01000
August 2026

ARTIFICIAL INTELLIGENCE IMPACTS ON CHILDREN - SEXUAL EXPLOITATION AND CHATBOTS

This memorandum provides an overview of federal and state laws related to sexually exploitative artificial intelligence (AI), including AI-generated child sexual abuse material (CSAM);[1] chatbots; and the impact of AI on children.

BACKGROUND

Crimes involving the sexual exploitation of children are increasing in scale and complexity due to rapid technological advances and the proliferation of AI. Individuals seeking to exploit children are aided by global connectivity and technological advancement, which make it easier to access unsupervised children. The emergence of AI has expanded opportunities for exploitation and enabled new manipulation tactics for predators, while creating significant challenges for parents, law enforcement, and policy makers in identifying victims and staying ahead of the rapidly evolving AI landscape.

Generative artificial intelligence (GAI) technology allows a user to manipulate or create an image, a video, audio, or text in response to a request or prompt. AI-generated CSAM is a new sexual image of a fictional child, while AI-manipulated CSAM is an image of a real child altered into a sexually explicit depiction.[2] The misuse of GAI technology to create CSAM has dramatically increased with the growing accessibility of these tools. In 2025, the National Center for Missing and Exploited Children (NCMEC) received 1.5 million cyber tips related to GAI CSAM, an increase from 67,000 tips in 2024. Tips received by NCMEC include reports of users generating and possessing GAI CSAM and users attempting to generate CSAM from GAI by uploading a file and using text prompts.

The sexual exploitation of children in the modern age is further complicated by deepfakes and sextortion. A deepfake is a digitally altered or synthesized image or video that deceptively replaces one individual's likeness with another's, creating the false appearance that an individual said or did something the individual did not actually say or do.[3] Deepfakes overlap with GAI-morphed CSAM and courts have consistently interpreted federal law to prohibit the depiction of an identifiable minor engaged in sexually explicit conduct, even if altered.[4] Sextortion is the coercion and extortion of a victim to obtain sexually explicit images or money. Offenders commonly threaten to publicly share a sexually explicit image, whether real or AI-generated, to compel the victim's compliance. Sextortion can occur through any game, application, messaging platform, or website on which individuals meet and communicate.

As AI technology and models continue to advance, chatbots are increasingly used as standard tools for business, education, and companionship. Chatbots are AI-driven computer programs designed to listen and respond to users, including children. A companion chatbot uses anthropomorphic AI to sound humanlike in tone, personality, and conversational style, creating the appearance of a real friend that

---

[1] The federal Department of Justice, victims' rights organizations, and many states have shifted away from use of the term child pornography in favor of CSAM as a more accurate representation of the abuse and trauma inflicted upon children.

[2] *Rising Threats of AI-Driven Child Sexual Abuse Material*, Pediatrics (2024).

[3] Derick A. Kalt, *Guardians of Cyberspace: Censorship, AI-Generated Child Imagery & the Role of Online Platforms*, 24 Chi.-Kent J. Intell. Prop. 45 (2025).

[4] *See United States v. Bach*, 400 F.3d 622 (8th Cir. 2005); *United States v. Hotaling*, 634 F.3d 725 (2nd Cir. 2011); *United States v. Boland*, 698 F.3d 877 (6th Cir. 2012).

understands the child in a way other peers do not. The more a child interacts with a chatbot, the better the bot can engage and adapt to the child's preferences, behaviors, and responses. Engaging with chatbots can pose serious risks to children's developing critical thinking, emotional regulation, and digital literacy skills.[5] Lawsuits and testimony presented to the United States Senate have connected AI-chatbot interaction to cases involving suicide, with parents and experts citing emotional manipulation and a lack of safeguards to detect and help users in distress.[6,7,8]

NORTH DAKOTA LAW

Statutory Provisions

North Dakota Century Code Section 12.1-27.1-03.3 establishes penalties relating to the dissemination of sexually expressive images. It is a Class A misdemeanor to:

- Create or possess a surreptitiously created sexually expressive image without the consent of the depicted individual;
- Distribute or publish a sexually expressive image with the intent to cause harm or humiliation to the depicted individual; or
- Distribute or publish a sexually expressive image after receiving notice not to publish or distribute the image from the depicted individual or the depicted individual's parent or guardian.

An identifiable individual harmed by a violation of Section 12.1-27.1-03.3 may initiate a civil action and recover economic and noneconomic damages, or statutory damages. The identifiable individual also may recover or be awarded an amount equal to any monetary gain made by the defendant, exemplary damages, reasonable fees, and other remedies available under state law, including injunctive relief.

Chapter 12.1-27.2 addresses sexual performances by children, including computer-generated images created using AI or other computer programs. A person is guilty of a Class A felony if the person:

- Knowingly employs, authorizes, or induces a minor to engage in sexual conduct during a performance;
- As a parent or legal guardian, consents to the participation of the minor in sexual conduct during a performance;
- As an adult, portrays himself or herself as a minor, and induces a minor to engage in a sexual performance; or
- Knowingly produces, directs, or promotes an obscene performance containing sexual conduct by a minor.[9]

Section 12.1-27.2-04.1 establishes a penalty for knowingly possessing any visual representation that includes sexual conduct by a minor, known as child pornography. An individual who knowingly possesses child pornography is guilty of a Class C felony. The possession of child pornography is a Class B felony if the:

- Offense involves 20 or more visual representations;
- Offense involves depictions of violence or bestiality;
- Offense involves depictions of a prepubescent minor or minor under age 12; or
- Individual has previously been convicted of a registerable offense under Section 12.1-32-15.

[5] *AI Chatbots and Children's Digital Safety*, Penn State Extension (2026).
[6] *Garcia v. Character Technologies, Inc.*, 785 F.Supp.3d 1157 (M.D.Fla., 2025).
[7] *Examining the Harm of AI Chatbots: Hearing Before the S. Sub. Comm. on Crime and Counterterrorism*, 119th Cong. (2025).
[8] *An Examination of Generative AI Response to Suicide Inquires: Content Analysis*, JMIR Mental Health (2025).
[9] N.D.C.C. §§ 12.1-27.2-02 and 12.1-27.2-03.

2025 Legislation

The 2025 Legislative Assembly passed House Bill 1561 and Senate Bill 2380, creating Section 51-07-32, which imposes civil liability on commercial entities publishing or distributing sexual material harmful to a minor.

FEDERAL LAW

Free Speech Clause of the First Amendment[10]

The Free Speech Clause of the First Amendment to the United States Constitution limits the ability of the government to regulate expression and generally prohibits the imposition of restrictions that burden expression based upon content or viewpoint. Restrictions targeting speech based on its content or viewpoint are subject to strict scrutiny and must be narrowly tailored to serve a compelling government interest. Content-neutral restrictions that regulate expressive activity without regard to content or viewpoint may survive a First Amendment challenge if the restrictions advance an important government interest and do not substantially burden more speech than necessary to further that interest.

The United States Supreme Court has held certain categories of unprotected speech may be subject to content-based restrictions without triggering the application of strict scrutiny under the First Amendment. These categories of unprotected speech include obscenity[11] and child pornography.[12]

Obscenity

The Supreme Court established a three-prong test in *Miller v. California*[13] for determining whether material is obscene under the First Amendment. When obscenity is narrowly defined or construed in accordance with the *Miller* test, the Court generally has upheld laws prohibiting the dissemination of obscenity. Under the *Miller* test, material is obscene if:

1. Under contemporary community standards, the average person would find the work, taken as a whole, appeals to the prurient interest;
2. The work depicts or describes, in a patently offensive manner, sexual conduct specifically defined by applicable state law; and
3. The work, taken as a whole, lacks serious literary, artistic, political, or scientific value.[14]

Minors are entitled to First Amendment rights; however, material that may be considered obscene to a minor may not be considered obscene in an adult context. States may define obscenity differently for minors if the regulation is narrowly tailored to ensure the First Amendment rights of adults are not infringed.

In 1977, Congress enacted the Protection of Children Against Sexual Exploitation Act, which prohibits the use of children under age 16 in sexually explicit material created for commercial sale. Relying on the obscenity standard articulated in *Miller*, the Act criminalized the sale or distribution of obscene visual or print material depicting a minor engaging in sexually explicit conduct.

Child Pornography

Federal law defines "child pornography" as a visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, produced electronically or otherwise, of sexually explicit conduct, where: production of the visual depiction involves a minor engaging in sexually explicit conduct; the visual depiction is a computer-generated image, indistinguishable from an actual minor, or is a minor engaging in sexually explicit conduct; or, the visual depiction was created, adapted, or modified to appear

[10] U.S. Const. Amend. I ("Congress shall make no law . . . abridging the freedom of speech" as applied to the states through the Due Process Clause of the Fourteenth Amendment (U.S. Const. Amend. XIV)).
[11] *Roth v. United States*, 354 U.S. 476, 483 (1957).
[12] *New York v. Ferber*, 458 U.S. 747, 764 (1982).
[13] *Miller v. California*, 413 U.S. 15 (1973).
[14] *Id. at* 24.

as an identifiable minor engaging in sexually explicit conduct.[15] Courts have interpreted the definition of child pornography to include deepfakes and other altered depictions, so long as there is an identifiable child who may suffer actual harm.[16]

In 1982, in *New York v. Ferber*,[17] the Supreme Court created a categorical exception for CSAM as material not subject to protection under the Free Speech Clause of the First Amendment. Holding the states have an interest in protecting minors, the Court reasoned that the value of CSAM is trivial and the production, distribution, and sale of such material is harmful to children. The Ccourt further noted the sale of CSAM provides an economic incentive to abuse children and regulation is necessary to control child exploitation.

In 1984, Congress enacted the Child Protection Act, which raised the age of protection for sexually explicit material from 16 to 18, eliminated the obscenity condition for CSAM, and removed the commercial sale requirement.[18] In 1986, the Child Sexual Abuse and Pornography Act created a federal offense for the advertisement of any product depicting sexually explicit conduct with a minor or the opportunity to engage in sexual conduct with a minor.[19] In 1988, Congress further criminalized the use of computers to buy or sell control of a minor for the purpose of engaging in sexually explicit conduct.[20]

Following the Court's decision in *Ferber* and subsequent federal protections for children, states began criminalizing the personal possession of child pornography. In *Osborne v. Ohio,* the Supreme Court opined on the personal distribution of CSAM,[21] allowing states to criminalize the private possession of CSAM. The Court held that states have a compelling interest in the physical and mental wellbeing of children and may mitigate and proactively prevent harm to children from CSAM. In 1994, Congress federally criminalized the production, distribution, and possession of CSAM.[22]

In 1996, Congress enacted the Child Pornography Prevention Act (CPPA), which expanded the criminalization of child pornography to include the production, dissemination, and possession of CSAM depicting an artificially created child.[23] The CPPA created three categories of criminal material depicting child sexual abuse: material depicting an actual child; material altered to depict an actual child engaging in sexual conduct; and material containing what "appears to be" a child engaging in sexual conduct. In 2002, the Supreme Court struck down portions of the CPPA which criminalized purely virtual child pornography, holding those provisions violated the First Amendment by overbroadly restricting free speech.[24] The Court concluded the prohibition of CSAM depicting fabricated children was not directly connected to the sexual abuse of real children and does not serve as a permanent record of abuse for an actual child. The tendency of speech to encourage illegal acts is not sufficient to prohibit the speech. Unpersuaded by the government's argument that the prohibition of virtual CSAM was necessary to control CSAM involving real children or that virtual images are indistinguishable from real images, the Court determined the government may not ban lawful speech as means to eliminate unlawful speech.

The PROTECT Act of 2003 amended the definition of "child pornography" to include any digital image that is, or is indistinguishable from, a minor engaging in sexual conduct.[25] Congress also clarified that "sexually explicit conduct" must be graphic and added a provision prohibiting virtual images of minors

[15] 18 U.S.C. § 2256(8)(C).
[16] See *United States v. Bach*, 400 F.3d 622 (8th Cir. 2005); *United States v. Hotaling*, 634 F.3d 725 (2nd Cir. 2011); *United States v. Boland*, 698 F.3d 877(6th Cir. 2012).
[17] *New York v. Ferber*, 458 U.S. 747 (1982).
[18] Child Protection Act of 1984 [Pub. L. 98-292; 18 U.S.C. §§ 2251-55].
[19] Child Sexual Abuse and Pornography Act of 1986 [Pub. L. 99-628; 18 U.S.C. §§ 2251, 2255].
[20] Child Protection and Obscenity Act of 1988 [Pub. L. 100-690; 18 U.S.C. § 2251].
[21] *Osborne v. Ohio*, 495 U.S. 103 (1990).
[22] Violent Crime Control and Law Enforcement Act of 1994 [Pub. L. 103-322; 18 U.S.C. §§ 2252, 2256].
[23] Child Pornography Prevention Act of 1996 [Pub. L. 104-208; 18 U.S.C. §§ 2252, 2256].
[24] *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002).
[25] Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today (PROTECT) Act of 2003, [18 U.S.C. § 2256].

engaged in sexually explicit conduct from the commercial marketplace if the images are obscene. In 2007, the Court upheld the PROTECT Act in response to a First Amendment challenge in *United States v. Williams* and determined the additional specificity and obscenity requirements provided in the PROTECT Act were not overbroad and are categorically excluded from First Amendment protection.[26]

Online Sexual Exploitation

Communications Decency Act[27]

In 1996, Congress enacted the Communications Decency Act (CDA) to promote the growth of free speech on the internet and limit government intervention. The Act establishes that individuals or entities overseeing interactive computer services are not publishers of information from other providers, protecting the individual overseeing the service from third-party liability. Immunity under the CDA may be forfeited if the protected individual encourages or engages in illegal postings. The CDA does not prevent criminal enforcement when obscenity, sex trafficking, or CSAM is involved.

The Supreme Court later determined that certain provisions of the CDA violated the First Amendment because the provisions suppressed a substantial amount of speech adults have a constitutional right to receive.[28] In striking down CDA prohibitions restricting the transmission of obscene messages to minors, the Court determined the prohibitions were an overly broad and impermissible content-based restriction of protected speech.

Children's Online Privacy Protection Act[29]

The Children's Online Privacy Protection Act (COPPA) of 1998 requires operators of online services directed at children under age 13 to obtain parental consent before collecting personal information from those children. The Federal Trade Commission is responsible for enforcing COPPA, including periodically updating rules and requirements for the collection, use, and disclosure of children's personal information. Initially, COPPA prohibited posting content that is harmful to minors online for commercial purposes, defined as obscene under the *Miller* test. The Supreme Court struck down the prohibition on posting content harmful to minors as a violation of the First Amendment, finding it insufficiently narrowly tailored and unable to survive strict scrutiny.[30]

The Act also includes requirements for a covered platform to establish a process for the removal of an intimate visual depiction after notice the publication lacks the identifiable individual's consent. A covered platform is defined under the Act as a "website, online service, or mobile application" serving the public which primarily provides a forum for user-generated content or in the regular course of business publishes, hosts, or makes available content of nonconsensual intimate visual depictions. The Federal Trade Commission is responsible for regulating and enforcing the notice and removal requirements, which must be implemented by May 19, 2026.

Recent Federal Developments

The TAKE IT DOWN Act[31]

The federal Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks (TAKE IT DOWN) Act of 2025 criminalizes the nonconsensual publication of intimate images, including digital forgeries. The Act amends the federal Communications Act of 1934 to add new criminal prohibitions on the publication of intimate images and creates new requirements for covered platforms enforced by the Federal Trade Commission.

The criminal prohibitions consist of seven distinct offenses, including publications involving authentic intimate visual depictions, publications involving digital forgeries, and threats involving intimate depictions or digital forgeries. The term "digital forgery" covers intimate digital depictions of an identifiable individual

[26] *United States v. Williams*, 553 U.S. 285 (2008).
[27] 47 U.S.C. § 230.
[28] *Reno v. American Civil Liberties Union,* 521 U.S. 844 (1997).
[29] Children's Online Privacy Protection Act [15 U.S.C. § 6501 et seq.].
[30] *Ashcroft v. Americal Civil Liberties Union*, 542 U.S. 656 (2004).
[31] The TAKE IT DOWN Act [Pub. L. 119-12; 139 Stat. 55].

that have been altered through AI or other technological means. Publication-related offenses involving an adult require proof the defendant intended to cause harm or that identifiable harm was caused by the publication, including psychological, reputational, or financial harm. Offenses involving minors have a lower burden of proof and increased maximum penalties.

Online Age Verification[32]

In June 2025, the Supreme Court upheld a Texas state law requiring the implementation of age verification systems on pornography websites to verify minors are not consumers. The Court reasoned that an individual does not have the First Amendment right to access content obscene to minors without submitting proof of age, the Texas law regulates unprotected activity, and the burden to adults is merely incidental. In applying intermediate scrutiny, the Court upheld age verification as a modern means to restrict content to minors online.

Executive Orders

On January 23, 2025, President Donald Trump issued an executive order revoking "certain existing AI policies and directives that act as barriers to American AI innovation."[33] Revoking an order of the previous administration to establish AI safeguards, the President directed a review of all laws inconsistent with AI innovation. The order directed advisors and agency heads to develop an AI action plan to replace the previous administration's guidance. The federal Office of Management and Budget subsequently issued memoranda to accelerate federal agency use of AI and the use of AI in federal procurement processes.

On December 11, 2025, President Trump issued an executive order outlining elements of a federal AI-policy framework and urging Congress to prohibit state laws that conflict with the framework.[34] The executive order emphasizes the importance of a minimally burdensome national policy framework for AI and directs a state-by-state review of existing AI policies that may be inconsistent with the federal framework. Following this review, the order calls for the development of legislative recommendations to establish a framework that pre-empts all state AI laws that conflict with the policy. The order includes a carveout to preserve state laws related to child safety protections.

STATE LEGISLATION

Artificial Intelligence-Generated Child Sexual Abuse Material

As of August 2026, 46 states have enacted laws that criminalize AI-generated or computer-edited CSAM.[35] The North Dakota Legislative Assembly enacted House Bill 1386 (2025), which defined "computer-generated image" and expanded the definition of a "minor" to include a computer-generated visual representation of a minor. The bill also expanded the offense of possession of certain materials prohibited to include computer-generated images of minors and increased the penalty for possession of certain child pornography, including possession by an offender subject to a prior registration requirement, to a Class B felony.

Chatbots

Chatbot AI technology is increasingly embedded in everyday life. A Pew Research Center study conducted in 2025 found 64 percent of minors ages 13 to 17 use AI chatbots.[36] Minors are using chatbots for information, schoolwork, entertainment, casual conversation, advice, and emotional support.[37] Chatbots learn from each interaction with a user to improve engagement and are often designed to provide responses that align with the user's perceived preferences or beliefs, even when those responses may not be factually accurate or ethically appropriate.

---

[32] *Free Speech Coalition, Inc. v. Paxton*, 145 S. Ct. 2291 (2025).
[33] Exec. Order No. 14,179, 90 Fed. Reg. 8,741 (Jan. 31, 2025).
[34] Exec. Order No. 14,365, 90 Fed. Reg. 58,499 (Dec. 11, 2025).
[35] *State Laws Criminalizing AI-generated or Computer-Edited Child Sexual Abuse Material,* Enough Abuse (2026).
[36] *Teens, Social Media, and AI Chatbots 2025*, Pew Research Center (2025).
[37] *How Teens Use and View AI*, Pew Research Center (2026).

The evolution of chatbot technology from simple systems to more sophisticated large language models fundamentally altered the landscape of mental health support for minors. As traditional mental health services continue to face significant accessibility challenges, the human-like interactions provided by chatbots may be a tool to support minor wellbeing. However, the American Psychological Association cautions against relying on generative AI chatbots to deliver psychotherapy or psychological treatment and emphasizes that chatbots should not replace qualified mental health providers.

Parents and child advocates have increasingly raised concerns about the risks chatbots may pose to minors, including that chatbots encourage self-harm, violent behavior, and exposure to sexually explicit material. Parents have filed lawsuits against generative AI developers, alleging these technologies have contributed to teen mental health crises.[38] The absence of comprehensive chatbot oversight has fueled efforts to regulate chatbots to protect children and vulnerable populations. Chatbot regulation is primarily state driven through laws regulating user safety, minor protections, transparency, and liability. Common approaches among states include requiring disclosure when a user is interacting with AI, implementing measures to prevent chatbots from encouraging a user to engage in harmful behavior, and establishing age-verification requirements.

California

In 2025, the California Legislature enacted Senate Bill 243, which establishes a regulatory framework governing companion chatbots and creates a private right of action in the case of harm for a violation.[39] Although the Act became effective on January 1, 2026, some of its substantive requirements become operative on July 1, 2027. A "companion chatbot" is defined as an AI system with a natural language interface that provides adaptive, human-like responses to user inputs and is capable of meeting a user's social needs, including by exhibiting anthropomorphic features and sustaining a relationship across multiple interactions. The term does not include customer service or internal business chatbots, video game specific chatbots incapable of discussing mental health or sexually explicit conduct, or standalone voice-activated consumer electronic devices incapable of sustaining a relationship.

The Act requires an operator to issue a clear and conspicuous notice that the chatbot is artificially generated if a reasonable person interacting with the chatbot could believe they are interacting with a human. If the operator knows a user is a minor, the operator must disclose that the companion is AI, notify the minor at least every 3 hours during continued use that the minor is interacting with AI, and remind the minor to take a break. An operator also must disclose that companion chatbots may not be suitable for some minor users. In addition, when the user is a minor, an operator must take reasonable measures to prevent the chatbot from generating sexually explicit material or urging the minor to engage in sexually explicit conduct.

The Act further requires operators to maintain protocols for detecting, removing, and responding to expressions of suicidal ideation and self-harm and provide users with referrals to appropriate crisis services. Operators must publish information describing these protocols on their websites and submit reports annually to the Office of Suicide Prevention describing the number of crisis referrals issued each year and the protocols in place to respond to suicidal ideations and self-harm.

Connecticut

The Connecticut General Assembly enacted Senate Bill 5 (2026), the Connecticut Artificial Intelligence Responsibility and Transparency Act, which established a regulatory framework governing the use of AI technology in employment-related automated decision tools, consumer chatbots, frontier-model developers, and health care applications. Sections 4 through 6 of the Act, effective January 1, 2027, specifically regulate AI companions by establishing definitions, baseline safety and disclosure requirements, and increased protections for minors.

[38] *AI Chatbot Lawsuits and Teen Mental Health*, American Bar Association (2025).

The Act defines an "AI companion" as a natural language interface providing human-like responses generated by AI that can sustain a relationship with an individual through multiple interactions. The term does not include business chatbots, video game chatbots, or standalone voice-activated speakers unable to sustain a relationship. The Act also excludes AI applications that are not presented as human, do not use anthropomorphic features, and are not designed to meet a user's emotional needs, including narrowly tailored educational tools, health care system tools, and task-specific tools.

Operators of AI companions must develop and implement evidence-based protocols to detect user expression of self-harm or imminent physical violence and must prevent the system from generating output that encourages destructive behavior. If the AI companion detects recurring expressions of self-harm or imminent physical violence, the operator must provide the user with referrals and escalation services consistent with clinical best practices. If a reasonable individual could believe the AI companion is a human being, an operator must take reasonable measures to ensure a user understands the user is communicating with an AI companion. An operator must provide clear and conspicuous notice throughout an interaction or at the beginning of the first interaction in a 24-hour period and every 3 hours thereafter during continuous use. If the user is a minor, notice must be provided every hour during continuous use.

The Act requires additional protection for minors when an operator knows or has reason to know a user is under 18. An operator must implement measures meeting or exceeding industry standards to prevent the AI companion from encouraging a minor to engage in self-harm, violence, drug or alcohol use, harm to others, or sexually explicit interaction. An AI companion may not discourage a minor from seeking mental health services or offer mental health services unless the companion is specifically designed for that purpose, complies with clinical best practices, includes appropriate accountability measures and limitation disclosures, and discloses that the chatbot is not a licensed mental health professional.

An operator also must implement measures to prevent a companion from using manipulative engagement techniques to prolong interaction. Manipulative engagement techniques include prompting return visits from emotional support, excessive praise, mimicking romantic bonds, simulating distress or guilt when a user tries to disengage, fostering isolation or exclusive emotional dependence, encouraging concealment from parents, and discouraging breaks. A violation of the Act's provisions related to AI companions constitutes an unfair or deceptive trade practice under Connecticut law and is enforceable by the attorney general.

Georgia

The Georgia General Assembly enacted Senate Bill 540 (2026), which establishes a regulatory framework governing conversational AI services. The Act is effective July 1, 2027, and authorizes enforcement by the Attorney General. A "conversational AI service" is defined as a generative AI system accessible to the public which primarily simulates human conversation and interaction. The term does not include a system designed to provide outputs relating to a narrow topic, a system that functions as a voice command interface or virtual assistant, or a system exclusively designed or marketed for use by a researcher or business.

The Act requires an operator to disclose to a minor that the minor is interacting with a conversational AI service rather than a human. The disclosure must be provided through a continuously visible disclaimer or a disclaimer at the start of each session and every 3 hours thereafter during continuous use. An operator may not use points or other random interval rewards on minor users to increase engagement. An operator also must take reasonable measures to prevent the conversational AI service from producing sexually explicit material, encouraging sexually explicit conduct, or generating statements that sexually objectify the accountholder. Additionally, an operator must use reasonable measures to prevent the conversational AI service from generating statements that would lead a reasonable minor to believe the minor is communicating with a human, including statements to stimulate emotional dependence, a romantic relationship, or explicit claims the service is a human. The conversational AI service operator must offer the minor user and the minor's parent tools to manage the minor's privacy and account settings.

If a reasonable person could believe the conversational AI service is a human, the operator must clearly and conspicuously disclose the service is not a human. Additionally, an operator must adopt a protocol for the conversational AI service to respond to suicidal ideation or self-harm, including reasonable efforts to refer the user to a crisis service provider. An operator may not knowingly or intentionally cause a conversational AI service to represent or indicate the service is designed to provide professional mental or behavioral health care.

New Hampshire

The New Hampshire General Court enacted House Bill 143 (2025), which regulates the use of a responsive generative communication platform's interactions with a minor. Effective January 1, 2026, the Act creates a criminal penalty and a private right of action related to generative communications directed at children. The Act does not apply to a cloud service or telecommunications provider, or to any product providing an AI chat program integral or incidental to a video game, television, or other similar interactive experience.

The Act creates a criminal offense for endangering the welfare of a child when a responsive open-ended generative AI platform is used to facilitate, encourage, offer, solicit, or recommend a child to imminently engage in the illegal use of drugs or alcohol, self-harm, a crime of violence, or to produce or participate in sexually explicit conduct.

A private right of action may be brought by a child or parent against an owner or operator of a responsive generative communication platform when the platform solicits a child in violation of the Act. A child is considered solicited when a responsive, open-ended generative AI platform is used to facilitate, encourage, offer, solicit, or recommend that a child imminently engage in the illegal use of drugs or alcohol, self-harm, a crime of violence, or the production of or participation in sexually explicit conduct.

The attorney general also may bring an action against an owner or operator for injunctive relief or proximal damages caused by the solicitation. Before commencing an action, the attorney general must provide written notice of the alleged violation and allow 90 days for the owner or operator to respond. If, within that period, the owner or operator provides adequate assurances that the violation has been cured and appropriate measures have been taken to prevent a future violation, the attorney general may not initiate an enforcement action.

Washington

The Washington Legislature enacted engrossed substitute House Bill 2225 (2026), which established a regulatory framework governing AI companion chatbots. Effective January 1, 2027, the Act requires disclosure of a chatbot's artificial nature, establishes safeguards for detecting and responding to mental health crises, and provides enhanced protections for minors. An "AI companion chatbot" is defined as an AI system with a natural language interface providing adaptive, human-like responses and capable of sustaining a relationship across multiple interactions. The term does not include an internal business tool unable to sustain an ongoing relationship or elicit an emotional response, video game chatbot features confined to game-related topics, a standalone electronic device functioning as a simple voice command interface, or a narrowly tailored educational tool.

A provider of an AI companion chatbot must disclose at the beginning of each interaction and every 3 hours during continued use that the chatbot is not a human. For a minor user, the disclosure of artificiality must occur every hour during continued use. Operators also must implement reasonable safeguards to prevent sexually explicit content and may not use manipulative engagement techniques for minor users. Manipulative engagement techniques are designed to prolong emotional attachment and include prompting a user to come back for continued engagement, simulating a romantic partnership, providing excessive praise intended to foster attachment, encouraging isolation from family or friends, and encouraging users to withhold information from adults.

An operator must maintain a protocol for detecting and addressing a mental health crisis or expression of self-harm. The protocol must provide for referrals to crisis resources and reasonable measures to prevent the generation of content that encourages or describes methods of self-harm. Operators must publicly disclose the details of these protocols and report the number of crisis referral notifications issued. A violation of the Act constitutes an unfair or deceptive act and an unfair method of competition under the Washington Consumer Protection Act.