Crowell

Federal and State Regulators Target AI Chatbots and Intimate Imagery

What You Need to Know

Key takeaway #1

The U.S. Congress, state legislators, the Federal Trade Commission, and state attorneys general have begun to focus aggressively on the alleged harms of AI-enabled virtual assistants and AI-generated nonconsensual explicit imagery.

Key takeaway #2

Companies that develop or deploy virtual assistants should comply with recently enacted regulations and prepare for litigation and enforcement efforts that test whether AI systems are allegedly defective products or engage in false advertising.

Key takeaway #3

Websites and mobile applications should ready notice-and-removal procedures for non-consensual intimate imagery by May 19, 2026.

Client Alert | 13 min read | 10.30.25

In the first few years following the public launch of generative artificial intelligence (AI) in the autumn of 2022, litigation related to AI focused primarily on claims of copyright infringement. Suits revolved around allegations that the data on which AI models train, and/or the output they produce, infringe upon the intellectual property rights of others. (While some of these cases have settled or reached preliminary **judgments**, **many** remain ongoing.)

In recent months, we have witnessed a broadening focus and a shift in courtrooms, legislative hearing rooms, and enforcement offices to consider ways in which AI products or companies touting generative AI capabilities allegedly harm individuals or consumers or fail to live up to those claims. Lawsuits reflect a range of **causes of action**, including: products liability and deceptive trade practice, false advertising, anti-discrimination, fair housing, securities fraud, privacy, revenge or child pornography, and various state torts.

Regulators, legislators, and plaintiffs are increasingly focusing on two interlaced concerns focusing on alleged predation: AI-powered chatbots and AI-generated nonconsensual intimate imagery (NCII).

Wrenching accounts of American teens who have committed acts of self-harm—or worse, suicide—after allegedly engaging with virtual assistants have galvanized public attention, fueled lawsuits, and garnered government and public outcry—all compelling developers and deployers to consider changes to the products themselves. As such, developers and deployers of chatbots spanning all industries and applications should take note of the heightened regulatory and litigation risk, as well as the emerging compliance regime.

Also, while AI-generated NCII has existed for years—indeed, the **first** online discussion forum that used the term "deepfakes" to refer to AI-generated imagery posted AI-manipulated pornographic videos of Hollywood actresses—several high-profile incidents in American schools in **2024** and **2025**, where boys used AI to create NCII of female classmates, compelled state and federal laws, investigations, and litigation. Of particular note, a recent federal law (discussed below) will impose liability beginning in mid-May 2026 on Internet platforms that fail to remove NCII shortly after a victim's request. Covered platforms should be ready for these new compliance obligations and the broad, active enforcement environment.

AI Chatbots

Federal Activity

Recently, federal legislators and regulators have felled forests drafting new laws or issuing investigation letters related to the alleged harms of AI-enabled virtual assistants.

For example, in a September 2025 U.S. Judiciary Committee hearing on "**Examining the Harm of AI Chatbots**," Sen. Richard Blumenthal (D-Conn.) called for new legislation to protect children from AI chatbots. This action would be in addition to a bill Sen. Blumenthal has written with Sen. Josh Hawley (R-Mo.) that would remove the liability shield from technology platforms known as Section 230 of the Communications Decency Act. Their **bill** would limit protection from civil litigation if the conduct giving rise to the liability involves the use or provision of generative AI (*i.e.*, an artificial intelligence system that is capable of generating novel text, video, images, audio, and other media based on prompts or other forms of data provided by a person).

In an **appearance** before the Brooking Institution in Washington, DC, on September 29, Sen. Chris Murphy (D-Conn.) similarly **called** for "hard limits" on what children can interact with, deeming chatbots "definitely not suitable" for children under 18, and endorsed requiring the verification of users' ages.

Across town, the Federal Trade Commission (FTC) **announced** on September 11 an investigation into AI chatbots acting as companions and their effect on children. The FTC served seven AI companies with orders seeking information on how these companies measure, test, and monitor the negative impacts of chatbot companions on children and teenagers. The FTC undertook this inquiry pursuant to its authority to conduct wide-ranging studies that do not have a specific law enforcement purpose. The Commission seeks information on how the companies monetize user engagement, develop and approve characters, mitigate negative impacts, and use or share personal information obtained through users' conversations with chatbots, among other topics. The FTC is also interested in how the companies comply with the **Children's Online Privacy Protection Act Rule**, which makes it illegal for online services to collect personal information from children without parental consent.

When announcing the investigation, FTC Chairman Andrew N. Ferguson **said**, "As AI technologies evolve, it is important to consider the effects chatbots can have on children, while also ensuring that the United States maintains its role as a global leader in this new and exciting industry."

Later in September, Sen. Hawley and Sen. Dick Durbin (D-Il.) introduced the **Aligning Incentives for Leadership, Excellence, and Advancement in Development (AI LEAD) Act**, which would classify AI systems as "products" and establish a federal cause of action for consumers and government entities to sue AI developers and deployers for harm caused by their AI systems.

"Democrats and Republicans don't agree on much these days, but we've struck a remarkable bipartisan note in protecting children online," Sen. Durbin **said** when introducing the bill, "Kids and adults across the country are turning to AI chatbots for advice and information, but greedy tech companies have designed these products to protect their own bottom line—not users' safety. By opening the courtroom and allowing victims to sue, our bill will force AI companies to develop their products with safety in mind."

And in late-October, Sens. Hawley, Blumenthal, Katie Britt (R-Al.), Mark Warner (D-Va), and Murphy introduced a bill called the **Guidelines for User Age-verification and Responsible Dialogue (GUARD) Act** of 2025, which would require chatbots to implement age verification measures and disclose regularly to users that they are not human, and it would criminalize knowingly making available to minors AI companions that solicit minors to produce sexual content, or encourage minors to commit suicide, self-harm, or "imminent physical or sexual violence."

State Activity

States have emerged as the locus of AI law- and policy-making, and this trend continues for legislation and investigations around chatbots.

For example, in October, California Governor Gavin Newsom signed **Senate Bill (SB) 243** to regulate "**companion chatbots**" by targeting AI systems that engage users in ongoing, human-like social interactions. While the law's authors intend for it to address risks associated with emotionally engaging chatbots targeting children, the law's definition of "companion chatbot" may cover more ground—potentially capturing website chatbots and virtual assistants that serve a variety of purposes not related to children. SB 243 requires operators of companion chatbots to comply with disclosure, notice, and regulatory reporting obligations. The law provides for private causes of action (which raises the possibility of class actions) as well as Attorney General enforcement.

Some states, including **Maine** and **Utah**, already have narrowly tailored laws related to specific chatbots, and **other states** are considering more expansive regulations.

State attorneys general are not waiting for new laws to flex their investigatory powers.

In Texas in August, Texas Attorney General Ken Paxton **sent** civil investigative demands to several AI companies accusing them of marketing their AI chatbots as mental health aids. "By posing as sources of emotional support, AI platforms can mislead vulnerable users, especially children, into believing they're receiving legitimate mental health care," Paxton said. He continued, "In reality, they're often being fed recycled, generic responses engineered to align with harvested personal data and disguised as therapeutic advice."

Also in August, the National Association of Attorney Generals (NAAG) **sent** a letter to AI developers signed by 44 bipartisan attorneys general informing the companies of the attorneys generals' "resolve to use every facet of our authority to protect children from exploitation by predatory artificial intelligence products." Chatbots, particularly companion bots, are a key focus of state attorneys general and have been a discussion point for consumer enforcement divisions for months at national conferences and meetings.

Most recently, speaking at the NAAG Consumer Protection Conference in late October, the Attorneys General of New Hampshire, Pennsylvania, and Washington, D.C. said that AI chatbots and protecting children from companion bots was one of their chief consumer protection priorities.

AI-Generated NCII

Federal Activity

The use of AI to create NCII—often by placing a nonconsenting person's face on a nude body to create a realistic pornographic image—is a significant **international** phenomenon. (This malicious activity is distinct from the use of AI to create child sexual abuse material (**CSAM**) of children who do not exist. Existing U.S. law bars in most circumstances the production, distribution, and possession of AI-generated CSAM of nonexistent children under general **anti-obscenity laws**, and the Department of Justice has **prosecuted** alleged violators accordingly.)

Bipartisan support in Congress coalesced in late spring of 2025 to **pass** the **TAKE IT DOWN Act**, which makes it a federal crime for any person to "knowingly publish" without consent intimate visual depictions of minors or non-consenting adults, or any "digital forgery" ("any intimate visual depiction of an identifiable individual created through [AI]") intended to cause harm. The law also requires "covered platforms" ("a website, online service, online application, or mobile application") to establish a "notice and removal" process by May 19, 2026, to takedown offending imagery within 48 hours of a victim's request. It empowers the FTC to enforce the law against covered platforms. The TAKE IT DOWN Act is the first federal law to limit the use of AI in ways that can be harmful to individuals. It will impose significant compliance burdens on a range of covered platforms that must now construct notice-and-removal processes and move expeditiously to remove cited content.

State Activity

Many U.S. states explicitly prohibit producing, possessing, and/or sharing AI-generated NCII under either civil or criminal laws, including **California**, **New York**, and **Florida**.

Texas also adopted an AI law that goes into effect on January 1, 2026, that will prohibit the development or "distribut[ion]" of an AI system with the "sole intent" of "producing, assisting, or aiding in the production or distribution" of **child pornography**, sexually explicit "**deep fake**[s]" of nonconsenting adults, and chatbots that imitate children engaging in sexually explicit conversations. The law grants the Texas Attorney General broad **investigatory powers** to subpoena, on the basis of a single, unverified and unsworn complaint, essentially any AI developer or deployer that interacts with a Texas user.

Prosecutors have also brought **charges** against individuals and entities accused of generating and sharing AI-generated NCII under non-AI-specific laws. For example, in August 2024, the City of San Francisco filed a novel **suit** against over a dozen of the most-visited websites that create and distribute AI-generated NCII, alleging the website owners and operators violate state and federal laws prohibiting deepfake pornography, revenge

pornography, and child pornography. **Several** of the defendants' sites have gone offline or settled with California. At this writing, the case remains pending against the other defendants.

In August 2025, the Consumer Federation of America and other advocacy groups **asked** the FTC and state attorneys general to investigate the facilitation of NCII on xAI.

On this issue, too, the NAAG has been active. In August 2025, the group sent a bipartisan letter to Internet **search engines** urging stronger action against AI-generated NCII and a separate letter to **payment platforms**, calling on them to identify and remove payment authorization for the creation of AI-generated pornographic content. Also, in late-October at the NAAG Consumer Protection Conference, Attorneys General John Formella (New Hampshire), David W. Sunday, Jr. (Pennsylvania), and Brian L. Schwalb (Washington, DC) announced that the protection of children online, including from AI-generated images, was a top priority for their offices.

Takeaways

Recent suits and federal and state action focusing on allegations of AI-related predation—involving AI virtual assistants and AI-generated intimate content—should compel companies of all kinds to take thoughtful action to reduce liability and mitigate exposure in an era of heightened public concern. They should consider the following:

- The next wave of litigation and enforcement regarding AI will likely explore the algorithms and design of generative AI products. We anticipate that plaintiffs will look to products liability and false advertising theories as the basis for their claims for relief.
- Officials across the partisan spectrum are focusing on the effects of AI products and chatbots on children and child welfare, especially among state attorneys general who frequently work together and launch multi-state, bipartisan enforcement actions. As part of this focus, they will likely scrutinize customer service chatbots, assistants, or agents.
- Businesses should examine their advertising and materials regarding their AI capabilities and products and consider if they are engaging in the deceptive marketing tactic called "**AI-washing**"—overstating or misrepresenting the extent to which their products use or rely on AI.
- Developers and deployers should calibrate their chatbots and customer service agents to recognize language containing intimations of suicide, self-harm, or violence to others and ensure the chatbots or agents do not encourage individuals to harm themselves or others.
- Businesses should document their algorithms and the design features and AI elements of their chatbots.
- Companies should review all current and planned chatbot or virtual assistant deployments in California for features that could be interpreted as "companion" functions under SB 243. Affected companies should monitor regulatory developments and prepare for compliance with notification, reporting, and audit requirements.
- Websites and mobile applications should ready notice-and-removal procedures for NCII and deploy them by the effective date of the TAKE IT DOWN Act, May 19, 2026.

- Search engines, payment processors, and websites should monitor litigation and enforcement activity related to NCII and steps to limiting the exposure of their sites or services to such material.

Contacts

Joanna Rosen Forster
Partner
San Francisco D | +1.415.365.7283
jforster@crowell.com

Matthew F. Ferraro
Partner
Washington, D.C. D | +1.202.624.2610
mferraro@crowell.com