wiley

ALERT

AI Chatbots: How to Address Five Key Legal Risks

November 24, 2025

Companies of all types are deploying chatbots using generative artificial intelligence (GenAI). While these tools offer significant potential benefits, they also present legal and regulatory risks that must be managed. GenAI chatbots are subject to a complex and growing patchwork of state and federal laws, facing scrutiny from both federal and state regulators. Below we identify five key risk areas that businesses should address as they deploy AI chatbots, as well as best practices to address these risks.

Five Key Risks to Address in Deploying AI Chatbots

1. Chatbots Are Subject to Disclosure and Transparency Requirements.

States have begun to implement AI laws that impose disclosure and transparency requirements on AI chatbots. These laws establish various requirements depending on the chatbots' functions. These include:

- Utah's AI Policy Act –which was recently amended—requires any person or entity employing GenAI to disclose to users that they are interacting with GenAI rather than a human, provided that the user makes a clear and unambiguous request. Additionally, individuals in regulated occupations, defined as those requiring a license or certification from the Utah Department of Commerce, must disclose the use of GenAI at the beginning of any "high-risk" interaction involving the provision of regulated services, such as healthcare, law, or finance.

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Alissa Lynwood
Associate
202.719.4527
alynwood@wiley.law

Kevin T. Nguyen
Associate
202.719.3395
knguyen@wiley.law

Practice Areas

Artificial Intelligence (AI)
Compliance
Federal Policy and Regulation
Privacy, Cyber & Data Governance
State Regulation

- The Colorado Artificial Intelligence Act (CAIA), currently set to take effect on June 30, 2026, mandates, among other requirements, that any deployer of a "high-risk" AI system must provide notice of "the types of high-risk [AI] systems that are currently deployed" and "how the deployer manages known or reasonably foreseeable risks of algorithmic discrimination that may arise." The CAIA also establishes disclosure requirements for any AI system that "is intended to interact with consumers," except for instances where "it would be obvious to a reasonable person that the person is interacting with an AI system."
- California's BOTS Act applies to automated bots on public-facing platforms with 10,000,000 or more unique monthly U.S. visitors within the past 12 months. The law requires companies deploying bots in certain circumstances to inform individuals with whom they communicate or interact with that they are interacting with automated bots. The law also prohibits deceptive misrepresentation about the bot's identity for the purpose of knowingly deceiving consumers about the content of the communication "to incentivize a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election."
- California Senate Bill No. 243 (SB 243), which will be effective on July 1, 2027, requires "companion" chatbot operators to disclose that users are interacting with these kinds of chatbots, implement protocols to prevent the dissemination of certain content (such as content relating to suicide, self-harm, or sexually explicit material), and provide annual reports to state authorities.

2. Chatbots May Trigger New Consumer Data Rights under California's ADMT Rules and State Privacy Law Opt-Outs.

The CCPA's newly finalized ADMT regulations establish regulatory requirements for the use of certain AI and automated tools, focusing on "high-risk" decision-making. The CCPA defines ADMT as "any technology that processes personal information and uses computation to replace human decision making or substantially replace human decision making." Under the CCPA regulations, beginning January 1, 2027, any business using a chatbot that qualifies as ADMT would be subject to key consumer rights requirements, including:

- Pre-Use Notice: Provide a prominent and conspicuous notice at or before the use of ADMT detailing the specific purpose for use, how the ADMT works, and the consumer's rights;
- Right to Opt Out: Provide consumers with the ability to opt out of the use of ADMT when the technology is used for what the regulations define as a "significant" decision; and
- Right to Access: Provide consumers with the right to access information about the ADMT's use.

In addition to the CCPA, many state comprehensive privacy laws grant consumers the right to opt out of certain automated profiling activities that produce legal or similarly significant effects. This may also impact chatbots performing certain kinds of functions regulated under these laws.

3. Chatbot Interactions with Children Face Increased Regulatory Focus and Require COPPA Compliance.

Government interest in chatbots interacting with children and teens has increased, and companies with chatbots will face questions about whether and how they interact with children and teens. Additionally, statutory privacy obligations apply to child and teen data.

- COPPA Compliance: Businesses must comply with the Children's Online Privacy Protection Act (COPPA) if they provide a service directed to children under 13, including if they have actual knowledge of collecting data from children under 13. COPPA requires parental notice and consent for certain data collection and sharing, and AI chatbot operators will need to assess whether COPPA requirements may apply.
- State Privacy Laws: Certain state privacy laws also extend privacy protections to teens between 13 and 18.
- FTC Inquiries: The FTC has issued 6(b) orders to companies operating AI chatbots as part of an information-gathering inquiry, signaling that the FTC may be looking closer at whether chatbot operators are engaged in any deceptive or unfair practices. The orders also include questions about chatbots used by children and teens, seeking information on any emotional influence and risk mitigation.

4. Businesses Face Liability for Misleading Chatbot Content.

Depending on the circumstances, companies may be held liable for their chatbots providing misleading information. Courts are likely to reject the defense that "AI did it," when companies have control over the AI tool. U.S. regulators have also begun to target deceptive AI practices under existing consumer protection laws.

- On the regulatory enforcement front, in *FTC v. DoNotPay, Inc.*, the FTC brought and settled deceptive advertising claims involving an AI chatbot marketed as a "robot lawyer" that could service as an adequate substitute for the expertise of a human lawyer. Although the chatbot generated legal documents and offered legal advice, it allegedly did so without validation or oversight, resulting in outputs that were not fit for legal use. The FTC alleged that DoNotPay's claims about its chatbot's capabilities were deceptive.

5. Chatbots Face Rising Litigation Risk Under State Wiretap Laws.

Companies using chatbots on their websites are facing private litigation, including class actions in states like California and Massachusetts, based on state wiretapping laws. These lawsuits often allege that chatbots record conversations and give third-party service providers access to communications without consent. Courts have ruled in different ways, but companies with chatbots should consider how to address potential legal risks. For example,

- *Jones v. Peloton*: In *Jones*, a California district court allowed CIPA claims to proceed past the pleading stage because the plaintiff described in detail how a third-party chatbot allegedly intercepted customer communications. The court treated the vendor as a potential "eavesdropper," signaling that plaintiffs

who can allege with specificity a technical interception mechanism may survive a motion to dismiss.

- *Gutierrez v. Converse*: The Ninth Circuit—through an unpublished, non-precedential decision—dismissed similar CIPA claims, finding no evidence of interception "while in transit" or use of a "telephone wire" as defined by the statute, and declined to decide whether CIPA applies to website chats. The case underscores how courts may interpret technical details and statutory language differently.

Best Practices for Proactive Risk Mitigation

Companies deploying AI chatbots should address these kinds of risks up front and evaluate their chatbots under their broader data governance and risk management programs. While different chatbot use cases will require various kinds of assessments, companies should consider a number of best practices including:

1. Conducting and maintaining an inventory of whether and how the organization is using chatbots, and what types of data the organization is collecting, using, and sharing through the operation or use of the chatbot.
2. Identifying what laws might apply to the particular chatbot use case, including any applicable federal laws as well as the growing patchwork of state laws and regulations, and developing a compliance strategy.
3. Establishing a risk management plan consistent with best practices. For example, the National Institute of Standards and Technology's AI Risk Management Framework (AI RMF) is a helpful tool to manage the risks of AI and is designed to be flexible in its implementation.
4. Appropriately vetting and managing third-party vendors supplying or supporting the chatbot, in order to help insulate the organization from potential liability.
5. Conducting ongoing testing and monitoring of AI systems and outputs to confirm that the chatbot is acting as intended and not acting in a way that will increase legal or regulatory risk.

***

Wiley's Artificial Intelligence Practice and Privacy, Cyber & Data Governance team counsels clients on compliance issues, risk management, and regulatory and policy approaches, and we engage with key government stakeholders in this quickly developing area. Please reach out to the authors with any questions.