SpencerFane®

# Before You Launch That AI Chatbot: Key Legal Risks and Practical Safeguards

AI chatbots have gone from novelty to necessity almost overnight. Whether embedded on a website, inside an app, or used internally to help employees find answers faster, these tools are now touching customer data, making suggestions, and sometimes sounding lot like a human advisor.

Regulators have noticed.

The Federal Trade Commission (FTC) has been clear that existing consumer protection laws apply fully to AI tools and has launched enforcement sweeps focused on deceptive AI claims and unfair practices.[1] In 2025, the FTC opened an inquiry into companies offering AI chatbots as "companions," specifically asking how they test and monitor potential harms to users, especially children and teens.[2]

If your business is thinking about deploying an AI chatbot, here are the key legal issues and practical safeguards to consider before you go live.

**Internal vs. Public Facing Chatbots: Different Risk Profiles**

Internal chatbots (for employees): these are typically used to search internal policies, summarize documents, or help with routine workflows. Key risks include:

- Exposure of confidential or regulated data (e.g., HR records, customer data, trade secrets)
- Employee monitoring issues if chat logs are used for performance evaluation
- Security and access controls if the chatbot is connected to internal systems.

Customer facing chatbots: these interact directly with customers or prospects, often without human review. Key risks include:

- Misleading or inaccurate statements about products, pricing, or legal/financial matters
- Unfair or deceptive practices under federal and state consumer protection laws
- Collection and use of personal data in ways that may conflict with state privacy laws
- Special risks if children or vulnerable users are likely to engage with the bot

Both types need guardrails, but public facing bots typically require more robust disclaimers, monitoring, and escalation paths.

**Core Legal Risk Areas for AI Chatbots**

Deceptive or misleading outputs include:

- Overstating what the chatbot can do ("guaranteed accurate," "certified financial advice") can be deceptive
- Allowing the chatbot to "hallucinate" about prices, terms, or performance can create misrepresentation risk.
- The FTC has signaled it will scrutinize AI claims and how companies market and deploy AI tools.

Data privacy and state privacy laws:

- Chatbots often collect names, contact information, inquiries, and sometimes sensitive or financial details if the user inputs that information.
- Comprehensive state privacy laws now exist in 20 U.S. states, creating obligations around notice, consumer rights, and data governance.

Children and teens:

- The FTC is particularly focused on AI used by or affecting minors, especially "companion" chatbots and emotionally manipulative features.
- If your service is directed to children or likely to attract minors, you may face additional obligations (e.g. COPPA, state children's privacy, and age-verification laws).

Confidentiality and intellectual property:

- If the bot is powered by a vendor's foundation model, you need clarity on:
  - Whether user inputs are used to train the model
  - Who owns outputs created using your proprietary data
  - How the vendor prevents leakage of confidential information

Security and abuse:

- Prompt injection, malicious links, and social engineering via chatbots can be security vectors
- Logs and training datasets may contain sensitive information that must be protected

**Disclaimers: What They Should Say and Where They Should Live**

Disclaimers will not fix a fundamentally unsafe deployment, but they are a key part of a defensible risk posture.

Content to consider:

- Nature of Service: disclose that the information provided by the chatbot does not constitute professional advice.
- No Professional Relationship: disclose that the use of the chatbot does not constitute a professional relationship.
- Accuracy Limits: disclose that the information provided by the chatbot may be incorrect and that the information provided is not a substitute for professional advice.
- Emergency and High-Risk Situations: advise that the chatbot should not be used to report emergencies or time sensitive issues.
- Privacy and Data Use: include a reference to how chat data is used and a link to your Privacy Policy and Terms of Service.

Placement and formatting:

- To avoid "dark pattern" concerns (where material terms are buried or obscured), regulators expect clear, prominent disclosure, not fine print at the bottom of the page.

Best practices include:

- A short, plain language notice directly above or next to the chat box, with a link to full terms.
- Reiterating key points in the chatbot's first automated message
- Using font size and contrast similar to the rest of the interface
- Requiring users to accept terms before using the chatbot

**Governance: Policy and Contract Checklist**

Before launching your chatbot, consider putting in place:

- An internal AI use policy for employees: explaining approved tools, prohibited uses, and escalation and reporting procedures.
- Vendor contracts that address: data processing obligation, limitations on training on your data, security standards and incident response, intellectual property ownership and licensing of model outputs, and indemnity and liability caps tailored to AI risk.
- Testing and monitoring practices aligned with regulator expectations: pre-launch testing for accuracy, bias, safety, and data leakage; ongoing monitoring and periodic audits of chat logs; and a process to quickly update guardrails as you learn from real world use.

*This blog was drafted by Jack Amaral, an attorney in the Minneapolis, Minnesota office of Spencer Fane. For more information, please visit www.spencerfane.com.*

—

1 https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes

2 https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-launches-inquiry-ai-chatbots-acting-companions