Insights, News & Events

10 BIGGEST MISTAKES BUSINESSES MAKE WHEN DEPLOYING AI CHATBOTS – AND 10 FIXES YOU CAN MAKE TODAY

Insights
Apr 13, 2026

10 Biggest Mistakes Businesses Make When Deploying AI Chatbots – And 10 Fixes You Can Make Today

Your business is probably already using AI-powered chatbots to handle customer service inquiries, screen job applicants, answer employee HR questions, and manage internal workflows. But legal exposure is growing fast, especially if your policies and oversight haven't caught up with your current usage. Regulators are writing new rules, plaintiffs' attorneys are testing new theories, and a patchwork of state laws is blooming across the country. Here are the most common mistakes businesses make when deploying AI chatbots, and the 10 fixes you can make today.

Mistake #1: Using "It's Just a Chatbot" as a Legal Defense

Many businesses utilize chatbots under the assumption that these tools are too routine to attract serious scrutiny. That assumption is no longer safe.

Washington just became the first state this year to sign a companion chatbot bill into law, with HB 2225 taking effect January 1, 2027. California's SB 243 and Maine's Chatbot Disclosure Act are already enforceable. Idaho and Georgia lawmakers passed chatbot bills just weeks ago. And bills in Arizona, Hawaii, Colorado, Michigan, Oklahoma, Maryland, and other states are advancing quickly through committees and floor votes.

Related People

Usama Kahf, CIPP/US
Partner

949.798.2118

David J. Walton, AIGP, CIPP/US
Partner

The Fix: Treat chatbot deployment as a legal and operational matter from day one. Assign cross-functional ownership across Legal, HR, and IT. Map your existing chatbot uses against the laws in effect in the states where you operate.

Mistake #2: Failing to Disclose That Users Are Talking to a Bot

Disclosure is the single most universal requirement across every state chatbot law enacted or currently pending. Most laws or bills require businesses to explicitly tell users they are interacting with AI, not a human. Washington's law, for example, mandates disclosure at the start of every interaction, with reminders every three hours for adult users and every hour for minors. California tracks closely. Other states have similar but not identical timing requirements.

But many businesses still don't do this. This happens especially with internal HR chatbots where companies believe that their own employees don't need to be told they are talking to a machine.

The Fix: Build disclosure into every chatbot interaction, internal and external, as a baseline practice regardless of where users are located. Use plain, conspicuous language before the conversation begins. Do not bury it in your terms of service. If your bot is used in multiple states, review the specific disclosure timing and format requirements for each.

Mistake #3: Overlooking Digital Wiretapping Liability

A wave of privacy litigation has emerged under state wiretapping laws, as plaintiffs' attorneys are arguing that chatbot vendors are recording conversations without adequate user consent. A federal court in Florida allowed a class action on exactly this theory to proceed in 2025, finding that user inputs captured by a healthcare organization's website chatbot could qualify as substantive communications, not mere technical data.

Florida cases involving website chatbots and tracking tools grew from five in 2021 to 28 in 2024, with hundreds filed in 2025 alone. California and other two-party consent states

610.230.6105

Service Focus

AI, Data, and Analytics

Digital Wiretapping Litigation

Litigation and Trials

Privacy and Cyber

Resource Hubs

AI Governance Hub

present similar risk. In class action scenarios involving thousands of website visitors, the statutory damages associated with such claims can add up quickly.

> **The Fix:** Audit every vendor whose tools touch your chatbot interactions, including analytics platforms, session replay tools, and live chat services. Implement clear, conspicuous consent notices before chatbot conversations begin. Consider active click-to-consent mechanisms rather than passive browsing-based acceptance. Also, we often find that businesses that agree to be featured as customers on a vendor's website offering a testimonial tend to get targeted for lawsuits first, so approach any such public arrangement with caution.

Mistake #4: Ignoring Data Privacy and Confidential Input Risks

Chatbots are data collection tools, whether businesses intend them to be or not. Every conversation generates inputs that may include personal information, health data, financial details. And, in the case of internal chatbots, that can include trade secrets, client strategy, and privileged communications.

- **Externally:** this dynamic means you must be concerned about data privacy statutes like CCPA, HIPAA (if you are a covered entity), and the growing body of state AI data regulations.
- **Internally:** the risk is employee behavior. Workers using an AI assistant might enter information that should never leave the organization. This could include client data, litigation strategy, unreleased financial results, and proprietary product information.
- **Additional risk:** AI chat histories can become litigation evidence. Two recent federal cases reached nearly opposite conclusions on whether employee interactions with AI tools are protected by attorney-client privilege or the work product doctrine, meaning the legal protection for those conversations is unsettled and jurisdiction-dependent. When employees use your chatbot to research a legal question, draft communications with a claimant, or discuss a personnel matter, those logs could end up in discovery. And remember, AI chatbot tools have robust

audit trails that track the conversation in detail, which can make for expensive fodder during discovery.

The Fix: For external chatbots, build a data flow map that documents what information is collected, where it goes, who can access it, and how long it is retained. Align your privacy disclosures with what actually happens. For internal chatbots, establish a clear written policy governing what employees may and may not input.

Mistake #5: Letting Chatbots Drift Into Employment Decisions

Employers are increasingly embedding chatbots in their HR operations, to screen resumes, answer benefits eligibility questions, route accommodation requests, schedule interviews, and more. But businesses often use them without fully considering whether they're influencing employment decisions. If they are, a new layer of legal exposure comes with it.

Title VII of the Civil Rights Act, the Americans with Disabilities Act, and the Age Discrimination in Employment Act all apply to automated tools that affect employment outcomes, just as they apply to human decision-makers. A chatbot that consistently routes certain candidates away from consideration (or that provides inconsistent information about benefits eligibility based on factors that correlate with protected characteristics, for example) can generate disparate impact liability.

On top of federal law, local and state requirements could soon be adding teeth. New York City's Local Law 144 requires employers using automated employment decision tools for hiring or promotion to conduct annual independent bias audits and publicly disclose the results. Other states, like Colorado, Illinois, and California, either currently or will soon regulate this field as well.

The Fix: Conduct an inventory of every chatbot that touches an HR function like hiring, performance, compensation, or discipline. Treat any tool that substantially assists or replaces discretionary employment decisions as an automated employment decision tool subject to applicable bias audit and disclosure requirements. Require human review before

any chatbot-influenced decision becomes final, and consider conducting a bias audit for every AI tool used during the hiring process.

Mistake #6: Ignoring the "Companion Creep" Problem

Washington, California, and other states have enacted laws that draw a legal line between a business-use chatbot (narrowly focused, transactional, exempt from the most stringent requirements) and a companion chatbot (defined broadly as any AI system capable of meeting a user's social needs through adaptive, human-like conversation).

What many businesses do not realize is that this line can move over time. A customer service bot trained on increasingly broad conversational data, or an internal HR bot that employees begin using for emotional support or personal guidance, can drift toward companion territory without any deliberate decision from the business. The bot that qualified for the business-use exemption on launch day may not qualify six months later.

The Fix: Monitor conversation logs periodically to assess whether your bot is being used in ways that go beyond its defined business purpose. Set guardrails in the system prompt or configuration that prohibit the chatbot from engaging with emotionally sensitive topics or sustaining relationship-building conversations. If you notice drift, address it in the bot's training and configuration. You'll also want to consult your FP counsel about whether your current deployment still qualifies for the business-use exemption in the states where you operate.

Mistake #7: No Human Escalation Protocols

What happens when a user's chatbot conversation takes a serious turn? A customer files a harassment complaint through your service portal. An employee asks your internal HR bot about mental health resources. A job applicant expresses distress during an AI-assisted screening interaction.

Many businesses have no defined answer to these questions or protocol for when and how a conversation

should be handed off to a human being. That gap creates both legal and human consequences.

Washington's new law requires companion chatbots to redirect users who raise topics like suicide or self-harm to mental health professionals, and California's law has similar requirements. But even for chatbots that qualify for the business-use exemption and are not subject to those laws, the practical and reputational stakes of a badly handled escalation are significant. Plaintiffs' lawyers would see an HR chatbot with no escalation protocol as a lawsuit waiting to materialize.

The Fix: Define clear escalation triggers for every chatbot deployment – specific topics or user signals that should route the conversation to a human immediately – and build those triggers into the bot's design. For internal HR chatbots in particular, ensure employees know how to reach a live person when they need one.

Mistake #8: Blind Vendor Reliance

Businesses routinely assume that compliance is the vendor's problem. After all, the vendor built the bot and runs the infrastructure. So if something goes wrong, the vendor is responsible... right? Wrong. This assumption is not always correct and potentially costly.

Under every chatbot law enacted to date, the deploying business carries legal responsibility for what the chatbot does, regardless of who developed it. And some vendor contracts contain broad disclaimers of liability that leave businesses using the AI holding the bag.

This is also where the wiretapping risk from Mistake #3 becomes a vendor contracting issue. If your chatbot vendor's tool is logging user conversations and that logging violates state wiretapping law, your company could be exposed. Whether you have contractual protection against that exposure depends entirely on what your agreement actually says.

The Fix: Treat chatbot vendor diligence as a legal matter, not just an IT procurement exercise. Before signing, review vendor contracts for data handling practices, security certifications, use-of-data restrictions

(including prohibitions on training models with your users' inputs), indemnification provisions, and explicit compliance representations. Insist on contractual clarity about who is responsible for disclosure mechanisms, consent collection, and incident response. Don't rely on the vendor's marketing materials as a substitute for contractual commitments. Follow our Essential Questions to Ask Your AI Vendor Before Deploying Artificial Intelligence at Your Organization guide, and consider how your vendor's data retention practices could affect your litigation posture.

Mistake #9: No Employee Policy or Training

Many businesses invest in chatbot tech, but then offer nothing for preparing their workforce to use it appropriately. The result is predictable: employees use the tool in ways the policy prohibits, they over-rely on outputs that deserve skepticism, or they simply do not know the rules at all.

There are two distinct failure modes here:

- The first is what goes in: employees inputting confidential data, privileged communications, or trade secrets into a third-party tool without understanding the consequences (see Mistake #4).
- The second is what comes out: employees treating AI-generated responses as definitive answers without verification, creating liability when those answers are wrong.

Both failure modes are avoidable, but only if businesses commit to actual training.

The Fix: Before any chatbot goes live, train employees on three things: what they are permitted to input, how to evaluate and verify outputs before acting on them, and how to escalate when something seems wrong. Make the policy concrete with examples rather than vague principles.

Mistake #10: Treating Deployment as a Finish Line

After a company introduces a chatbot, the deployment team often moves on. No one owns ongoing oversight, and the

bot runs on autopilot until something goes wrong. But launching the product is not the end of the process, because chatbots are not static.

Conversation patterns shift. Training data evolves. Vendors update their technology stacks. Laws take effect in new states. The compliance posture of your chatbot on launch day may look nothing like its compliance posture a year later. Without monitoring, you will not know until a regulator or plaintiffs' attorney tells you.

The Fix: Assign ongoing ownership of each chatbot launch to a named individual or cross-functional team with the authority to take action when something needs to change. Establish a periodic review schedule that covers conversation log audits, policy alignment checks, vendor contract reviews, and regulatory updates across all states where you operate. Build an incident response protocol so that when something does go wrong, the response is organized rather than improvised.

Conclusion

We will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our AI, Data, and Analytics Practice Group.