The Computer & Internet Lawyer

Volume 40 ▲ Number 9 ▲ October 2023

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Customer Service Chatbots: What You Need To Know

By Katherine White, Ioana Gorecki and Whitney M. Smith

Generative AI continues to dominate the conversation in 2023, and one particular aspect receiving increased scrutiny in the past weeks is AI-powered customer service chatbots. The Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC) have both raised concerns about replacing human customer service agents with sophisticated large language models (LLMs), ranging from their limited ability to solve complex problems, the potential for inaccurate information, the use of "dark patterns," and privacy and data security concerns regarding customers' inputted data or data collected and used to train the algorithms.

In addition, there have been recent class actions alleging chatbots violate the California Invasion of Privacy Act (CIPA), California's wiretapping law.

The following "Best Practices" offer a practical guide to implementing a compliant customer service chatbot into your business.

The authors, attorneys with Kelley Drye & Warren LLP, may be contacted at kwhite@kelleydrye.com, igorecki@kelleydrye.com and wsmith@kelleydrye.com, respectively.

1. PICK THE RIGHT TECHNOLOGY THAT WILL SUPPORT, NOT FRUSTRATE, YOUR CUSTOMERS

Customer service chatbots that cannot understand consumer requests, require the use of particular phrases to trigger resolution, force customers to jump through multiple hoops to obtain information, or fail to connect customers with a live agent when needed may create more problems than they solve and trigger regulatory scrutiny. The CFPB has warned companies that over-reliance on chatbots can result in inadequate levels of customer assistance due to the technology's limited ability to solve complex problems. This can be particularly problematic in areas where the lack of reliable assistance could have a significant detrimental impact on consumers' lives (for example, in the health or financial contexts). This is why it is extremely important to select chatbot technology that is well-suited to your customer service needs. Current technology offerings vary substantially in terms of sophistication, automation, and features. The less capable the chatbot technology, the more important it is to ensure that human customer service agents are on standby to resolve customers' concerns.

2. DO NOT HIDE THE BALL

Consumers should always know when they are interacting with a chatbot instead of a live agent. For less sensitive use cases, if chatbots are your primary form of customer service and consumers are likely to have only limited access to live agents, disclose this fact up front, before customers sign up for your services. It is important that consumers understand if using a service will limit their ability to connect with live agents, so they consider tradeoffs and can make an informed choice. The CFPB has noted that lack of access to a human customer service representative may not be apparent until consumers experience an issue and must invest time and effort into resolving it. The failure to disclose such practice may be viewed as an unfair practice or as undercutting competition for institutions that do invest in meaningful and effective customer support.

Further, if the responses or recommendations provided through a chatbot are motivated by any commercial connection (such as native advertising), make sure to disclose that up front.

The FTC is particularly concerned about "dark patterns" within the context of AI technologies, noting that consumers often place too much trust in machines and expect AI-generated recommendations or advice to be neutral and accurate. As a result, make sure your chatbot doesn't steer or manipulate customers into decisions that may not be in their best interests, such as recommending the highest-cost product in a range solely in order to get customers to pay more. The FTC has said that using such practices, especially in the areas of finance, health, education, housing, or employment, is likely to be an unfair or deceptive act or practice under the FTC Act.

Despite the technological advances, remember that chatbots are still limited in many ways in their ability to understand and solve complex customer problems. For complex issues, or sensitive contexts, such as financial, health, education, housing, or employment, ensure that consumers still have a way to request connection to a live agent without having to jump through multiple hoops or face a lengthy wait time. Backing up chatbot systems with a robust live customer service program will ensure that more complex problems are addressed in a timely manner and without undue consumer frustration.

3. MONITOR FOR FALSE OR INCORRECT INFORMATION

Remember that companies will be held responsible for anything their AI chatbots say to customers. If anything goes wrong, the FTC says you cannot blame a third-party developer of the technology or escape responsibility because the technology is a "black box" that you don't understand or know how to test. Making sure chatbots are giving out correct information is particularly important in sensitive contexts.

For example, financial institutions must provide consumers with certain information that is legally required to be accurate, and any lapses could constitute law violations.

Similarly, in the health context, making false health claims or providing consumers with inaccurate health guidance could have significant negative repercussions.

Other high-risk areas are education, housing, and employment. Make sure you regularly monitor the chatbot, so you can flag any incorrect or problematic responses.

In addition, you can minimize risk by programming the chatbot to refer all questions or requests of a more sensitive nature or pertaining to legal requirements to a human agent for review.

4. COMPLY WITH RELEVANT STATUTES

Just as you are responsible for everything your chatbot says to customers, you are responsible for ensuring that your AI chatbot is compliant with existing laws and regulations. For example, if the chatbot is collecting personal data from customers, it must comply with applicable privacy laws. If your chatbot is used to help enroll consumers for a subscription service, it must comply with relevant auto-renewal laws, such as the Restore Online Shoppers' Confidence Act (ROSCA). If you are an online marketplace and you are using a chatbot to field complaints about suspicious activity, you must comply with the INFORM Consumers Act. If you are covered by the Gramm-Leach-Bliley Act, you must ensure that your safeguards extend to information collected by the chatbot. If you operate in California, you must ensure you comply with its law prohibiting knowingly deceiving consumers by using bots to incentivize a sale or influence a vote in an election by clearly disclosing your use of a bot to consumers. Regulators throughout government have been clear that they are focused on ensuring that the use of AI complies with existing law, and will not hesitate to take enforcement action where warranted.

It is not just regulators that are paying attention to this space, but private litigants as well. In particular, we

have seen a wave of lawsuits filed under California's Invasion of Privacy Act (CIPA) predicated upon alleged interactions with chatbot technology on websites. CIPA provides for statutory damages in the amount of $5,000 per violation and these claims are often filed as putative class actions, where exposure can quickly add up. You can mitigate the risk of these types of claims with a simple disclosure when a user starts to engage with your chat feature, letting them know that chat sessions may be monitored and recorded and providing a link to your privacy policy.

5. TEST YOUR CHATBOT FOR BIASED RESULTS OR UNFAIR OUTCOMES

Generative AI is trained on significant amounts of data, some of which could contain explicit or implicit biases, resulting in biased or discriminatory responses and results. Before deployment, test your chatbot to ensure that it does not result in discriminatory outcomes for certain groups. This is key if your chatbot will be used in the context of financial, credit, employment, or housing transactions that are covered by antidiscrimination laws.

Other discriminatory results, such as targeted advertising that uses race, color, religion and sex as bases could be viewed by the FTC as an unfair practice. As with false or incorrect statements, a company cannot simply blame the third-party developer or claim they did not intend to create discriminatory outcomes. You need to ask the right questions about the types of data used to build the AI model, test the model before deployment, and continue to monitor and periodically test the system to make sure it doesn't discriminate on the basis of race, gender, or other protected classes.

6. CHATBOT-TRAINING DATA SETS MUST BE LAWFULLY COLLECTED AND USED

Generative AI depends on vast amounts of data, and it is important to ensure that you have any necessary permissions before you use data to train and improve your model. Be sure that you have proper licensure before using trademarked or copyrighted materials, so you can avoid lawsuits for infringing IP. In addition, with the proliferation of international and state privacy laws, it is important to ensure that you have the requisite legal basis or consent to use any personal data in your AI models, and that such use is consistent with your privacy representations and privacy policy.

7. SAFEGUARD CUSTOMERS FROM DATA BREACHES

As with any other technology, if you are using AI in chatbots to collect personal data from consumers, you are obligated to safeguard that information. You must take reasonable steps to protect the confidentiality, integrity, and security of that information. What qualifies as reasonable depends on the nature of your business and the sensitivity of the information.

Best practices include employing end-to-end encryption for customer information, and periodic testing for vulnerabilities. You should conduct due diligence on any vendor for the chatbot technology to mitigate the risk of the chatbot being used as a vector for compromise.

In addition, ensure that you require proper authentication and authorization for the chatbot to reduce the risk that malicious actors can impersonate the chatbot and trick consumers into providing them with sensitive information.