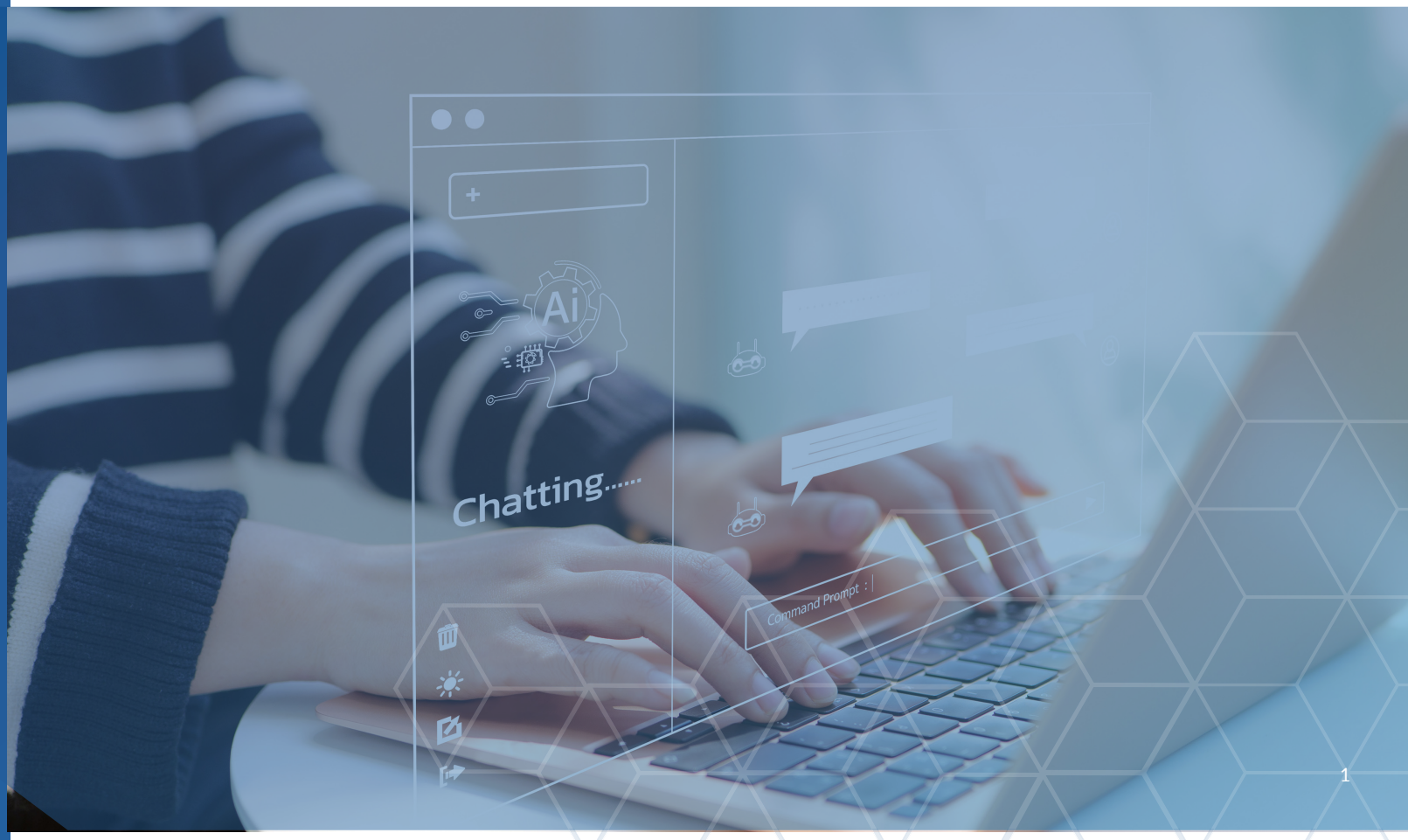
Advising Businesses on AI-Powered Chatbot Use: Key Considerations for California Lawyers

They used to be simple customer service tools, but advances in generative artificial intelligence (AI) have propelled some chatbots to the status of sophisticated digital assistants. In the two years since ChatGPT made its debut, all industries have raced to discover how they can implement chatbot technology to streamline operations and enhance customer engagement.

But with increased functionality comes greater risk. The more integral these AI-powered tools become to industries, the more important it is for California attorneys to advise businesses on their legal obligations when deploying them. Whether a client seeks to streamline customer interactions or offer around-the-clock service, there are several critical areas to address to mitigate risks and maintain compliance regardless of whether their business is based in California.



1-800-232-3444 www.ceb.com

Here's what lawyers need to know:

1. Protecting customer information is paramount

Anytime chatbots interact directly with the public, data privacy and security should become top priorities. Clients must be mindful of what data their chatbot collects, especially if it includes personally identifiable information or sensitive details, such as Social Security numbers or payment details.

When advising clients on data management for chatbot interactions, consider the following factors:

What type of data is being collected?

Chatbots often gather names, contact details and sensitive information. If users are sharing anything personally identifiable, privacy protocols should be stringent.

The California Consumer Privacy Act (CCPA) governs the use of this information, outlining how to safeguard it and inform users of their rights. Implementing these protections is important not only for compliance purposes but also for building trust — reassuring customers that their data is being handled responsibly.

The CCPA applies to all for-profit legal entities doing business in California that collect consumers' personal information, control how it's used and either have a gross annual revenue of more than $25 million or process the personal information of at least 50,000 consumers, households or devices for commercial purposes. Violations can trigger attorney general enforcement actions, resulting in injunctions and civil penalties of up to $2,500 per violation or $7,500 per intentional violation.

What security measures are in place?

The CCPA requires businesses to give notice to consumers regarding the use of their personal information and provide a way for them to exercise their rights. This means clients should be prepared to respond to data access, deletion and opt-out requests.

Is it clear to consumers that they're interacting with a chatbot?

California's Bot Disclosure Law is centered around transparency and user trust, mandating that businesses must inform users they're interacting with an automated system rather than a human.

For this reason, your client should have a privacy policy that explicitly discloses when a chatbot is being used, what data is being collected and how it will be managed and protected. This is not only important for complying with California law, but also with the European Union's General Data Protection Regulation (GDPR), which applies to any business that processes the data of EU citizens. Most privacy disputes arise from businesses failing to properly explain how they're using people's information.

2. Think beyond California

Such is the nature of the internet that chatbot interactions are rarely confined to any one region — and neither should your legal advice. Many businesses interact with customers across state or national borders, which triggers a host of compliance considerations spanning various jurisdictions.

If your client operates nationally or internationally, help them develop multijurisdictional compliance strategies to ensure they meet the requirements of every region where they do business. This could include complying with the GDPR, the Children's Online Privacy Protection Act, the Electronic Communications Privacy Act, the Federal Trade Commission Act (which enforces privacy protections by prohibiting unfair or deceptive practices) and various state-specific privacy laws.

3. Account for sector-specific rules

The focus of your client's business can shape their obligations when implementing chatbots, and sometimes additional layers of compliance are needed.

Examples include the Health Insurance Portability and Accountability Act (HIPAA), which governs the protection of personal health information. Chatbots handling any medical or health-related data must abide by strict confidentiality and data protection requirements. Similarly, chatbots operating in the financial services sector could be subject to the Gramm-Leach-Bliley Act (GLBA), which says financial institutions must safeguard consumers' information and have specific privacy notices and data security provisions.

Make sure clients are clear on which regulations apply to the type of information their chatbot will manage, and recommend tailored compliance strategies. This could include safeguards or restrictions on the types of data the chatbot collects.

4. Minimize misinformation with testing and training

While generative AI chatbots have the potential to improve the user experience, their responses can produce inaccurate or outdated information — especially if sourced from incorrect or biased datasets. Businesses should consider implementing regular training and updates to the chatbot's underlying algorithms, ensuring it pulls data from reliable, up-to-date sources. This is crucial if the chatbot gives advice or information about legal, financial or health implications.

By establishing a clear process for spotting and correcting inaccuracies, your client can maintain credibility and reduce the risk of misinformation. This might include disclaimers and other transparency measures. For example, chatbots giving health-related information should clarify that they don't replace professional medical advice. Human oversight and regular audits of the data the chatbot accesses can also ensure the system stays accurate and reliable.

5. Learn from past incidents

History has a way of reminding us that even the most well-intentioned innovations can falter without careful oversight. By studying the infamous chatbot shortcomings of yesterday, you can help your clients avoid costly missteps — and the headlines.

A notable example comes from Air Canada, which faced legal trouble and public embarrassment after its chatbot promised one passenger a discount that **didn't exist**.

Among the most financially damaging was an incident involving Sephora, which **agreed to pay a $1.2 million fine** to settle a CCPA lawsuit. California Attorney General Rob Bonta alleged the company failed to disclose that it sold the personal data collected via its website and didn't provide the necessary opt-out requests from users.

Cases like these underscore the need for regular evaluations of chatbot accuracy. Encourage your clients to learn from them by testing chatbot responses for varied and complex scenarios and adjusting them where necessary.

The golden rule for chatbots

Anytime a client's chatbot interacts with the public, disclosure should be your guiding principle. By prioritizing transparency, understanding all applicable regulations and establishing processes for addressing inaccuracies and other issues, clients can build trust with their customer base while safeguarding data and avoid becoming the next cautionary tale.

At CEB, we believe AI is a transformative and exciting technology for the legal profession, but attorneys remain the primary content creators and curators of our legal content and offerings. Get in touch to **schedule a free demo**.