



Custom ChatGPTs: Navigating Legal and Ethical Compliance for Public-Facing AI Tools

By Carolyn Elefant

Abstract

This article explores the legal and ethical considerations lawyers must address when creating custom versions of ChatGPT for public use. It discusses the potential applications of these tools, such as educating clients on legal matters or providing preliminary advice to landlords. The article outlines key ethical requirements, including AI disclosure, supervision, attorney-client relationship, confidentiality, and unauthorized practice of law (UPL). It also examines legal and business concerns related to licensing, training materials, and liability for inaccurate responses. Through a review of state ethics guidelines and expert opinions, the article offers practical solutions to ensure compliance and protect both users and legal practitioners.

So, you want to build and launch a [custom version of Chat GPT](#) to share with your law firm's clients. Maybe you want to create a platform trained on your firm's extensive database of Colorado child support cases to educate clients on factors that courts may apply in modifying an existing arrangement. Or maybe you want to respond to questions from mom-and-pop landlords about evicting a lessee who won't pay, or offer a checklist on documents to gather for a lawsuit after being rear-ended in an auto accident.

With ChatGPT custom tools, the possibilities to create a tool to expand access to justice, educate the public or generate leads are endless. But what's also endless are the myriad of legal and ethics questions raised when lawyers create custom GPTs for use by the public. So here's a quick list of issues and solutions if you choose to build a public-facing GPT.

I. Legal Ethics Requirements

Sources: Ethics guidance from [California](#), [Florida](#), [New Jersey](#), [NYSBA](#), [North Carolina](#), [Pennsylvania](#) and [Kentucky](#).

- **AI Disclosure Requirements:** Several states require disclosure of AI use to clients, or clarification that a chat-bot is machine and not human. An easy fix: use the custom GPT instructions to deliver an appropriate disclosure when users submit a request.
- **Duty to Supervise:** Most states require lawyers to supervise and oversee AI use. But how to supervise a public-facing GPT when the sponsoring firm can't monitor either queries received or responses delivered? One option: constantly test the GPT with queries anticipated from users and iterate revisions as needed. And as further protection, warn users that the GPT results aren't monitored for accuracy and can't be relied on without consulting with a lawyer. Together, ongoing testing and disclosure of lack of monitoring should suffice to discharge the duty to supervise obligation.
- **Attorney-Client Relationship and Confidentiality:** As with any interactive web form or chat bot, a public GPT should clarify that no attorney client relationship is formed

when a query is submitted. And to ensure preservation of confidentiality, a GPT should caution users against submitting detailed personal information.

- **Unauthorized Practice of Law:** [Sources: Joseph Avery et. al., [Chat GPT Esq.: Recasting UPL in an AI Age](#) (2024); Ed Walters, [Regulating UPL in an Age of AI](#) (2024); Thomas Spahn, [Is Your AI Guilty of UPL?](#) (2018)] Does a custom ChatGPT constitute unauthorized practice of law. Most experts concur that the law is unclear, though it bears noting that most UPL statutes expressly refer to persons engaged in law practice, not machines. That said, Ed Walters’s article suggests that software products may be insulated from UPL violations with clear disclaimers that they provide general information, not advice and make clear that responses are generated by a machine, not a live attorney.

I. Legal and Business Considerations

- **Licenses and Training Material:** Lawyers can upload caselaw, statutes and all kinds of practice materials to train and refine custom GPTs. But it’s important to review the terms of licenses covering third-party materials like treatises or CLE content that you may want to include. Fortunately, few resources outright prohibit their use for AI-training...yet. Absent an express prohibition on use for training, courts would evaluate whether the content produced is derivative of the training material – an issue now wending its way through the courts. For added protection, custom GPTs can be instructed not to spew out word-for-word content from training material. Finally, if all else fails, bear in mind that [Open AI has promised to defend customers against copyright claims](#).
- **Privacy of Training Materials:** It goes without saying that lawyers shouldn’t use confidential client materials for training. That said, lawyers may want to train custom GPTs on internal, proprietary content developed by the firm that they don’t want OpenAI to access for its own training. Fortunately, Open AI offers a privacy option to protect content uploaded for training – and there are other technical hacks to prevent users from reverse-engineering your custom GPT.
- **Liability for Inaccurate Responses** Recently, [Canada Air was required to honor a fare](#) that its chatbot erroneously provided to a customer. Similar cases are likely as consumers [overwhelmingly believe](#) that the company sponsoring the chatbot and not the technology is to blame for errors. Here again, clear disclosures that results may not be accurate coupled with warnings to consult with an attorney before taking action can help ward off liability.

Conclusion

Creating a custom ChatGPT for public use offers significant potential to expand access to legal information and generate client leads. However, it also presents a complex array of legal and ethical challenges. Lawyers must ensure proper AI disclosure, maintain oversight to fulfill their duty to supervise, and clearly communicate that no attorney-client relationship is formed through the tool. Additionally, safeguards must be implemented to avoid

unauthorized practice of law and protect confidentiality. By addressing these issues and incorporating robust disclaimers, legal professionals can responsibly leverage AI technology to enhance their services while mitigating risks.