TheFormTool LLC

Legal Privilege, Cloud AI and the Ethics Gap in Document Automation

Generative AI tools like ChatGPT are increasingly being used by legal professionals for drafting, brainstorming, and research. An increasing number of document automation vendors in the legal industry are integrating generative AI or cloud-based services into their offerings. But these tools are not confidential—and their use poses a serious risk to attorney-client privilege, regulatory compliance, and ethical obligations. Recent developments indicate serious trouble may lie ahead.

It's time for lawyers, law firms, bar associations, and anyone handling confidential data—or subject to CCPA, HIPAA, or GDPR—to look beyond hardware and encryption and ask the foundational question: ***once data is shared with the cloud, who really owns and controls it?***

TheFormTool LLC
www.theformtool.com
info@theformtool.com

© TheFormTool, LLC

Executive Summary

Generative AI tools like ChatGPT are increasingly being used by legal professionals for drafting, brainstorming, and research. But these tools are not confidential—and their use poses a serious risk to attorney-client privilege, regulatory compliance, and ethical obligations.

Recent revelations by OpenAI CEO Sam Altman and a federal court order requiring the indefinite retention of ChatGPT user logs have made one fact unavoidable: cloud-based AI tools do not offer legal privilege or confidentiality protection.

This concern extends beyond general-purpose tools like ChatGPT. An increasing number of document automation vendors in the legal industry are integrating generative AI or cloud-based services into their offerings. While marketed as productivity boosters, these features often come at the cost of diminished confidentiality and uncertain privilege protections.

This white paper explains the implications of this gap for lawyers, regulators, and the public, and it presents a viable alternative: secure, offline document automation that keeps sensitive data fully under user control. It concludes with concrete recommendations for Bar associations and ethics committees to protect privilege in the age of AI.

What OpenAI's Sam Altman Said

*"People talk about the most personal sh** in their lives to ChatGPT. […] And right now, if you talk to a therapist or a lawyer or a doctor about those problems, there's legal privilege for it. […] We haven't figured that out yet for when you talk to ChatGPT."*

What Sam Altman Just Admitted

In July 2025, OpenAI CEO Sam Altman made headlines with a candid acknowledgment:

*"People talk about the most personal sh** in their lives to ChatGPT. […] And right now, if you talk to a therapist or a lawyer or a doctor about those problems, there's legal privilege for it. […] We haven't figured that out yet for when you talk to ChatGPT."*

This was not a leak or legal filing—it was a public statement from the head of the company that created ChatGPT. It underscored what legal ethicists have warned for over two years (including TheFormTool, LLC): communications with generative AI tools are not protected.

No legal privilege. No confidentiality. No guaranteed deletion.

The result is clear: attorneys using public AI tools—even for drafting or internal notes—are likely placing sensitive client data at risk of exposure, subpoena, or discovery.

© TheFormTool, LLC

Legal Ethics: Where the Cloud Falls Short

Confidentiality and data protection are cornerstones of legal practice. These obligations are codified in:

ABA Model Rule 1.6: requires lawyers to preserve the confidentiality of client information.

State Professional Conduct Rules: mirror or extend these duties.

Privacy Laws: such as CCPA, HIPAA, and GDPR, which regulate how data is stored, transferred, and accessed.

Cloud-based AI platforms—whether general (ChatGPT) or legal-specific (e.g., Gavel, Lawyaw)—introduce uncertainty into all of these areas:

- Data may be stored on third-party or foreign servers
- Vendors may reserve rights to monitor or audit usage
- Even opt-out deletion controls may be overridden by court order

These concerns are compounded when vendors add AI features that silently transmit content to cloud processors without the lawyer's knowledge or meaningful consent.

The False Sense of Privacy in GenAI Tools

Since early 2023, legal commentators have warned that using ChatGPT may breach privilege.

- **March 2024**: A loophole in Microsoft Azure's Open AI abuse monitoring allowed employee access to prompt/response logs.
- **July 2025**: A federal judge ordered Open AI to preserve all user logs indefinitely—even those from users who had opted for permanent deletion.

The implication: lawyers who use these tools may be unknowingly creating discoverable content outside their control.

The safer rule of thumb? Treat anything input into a public GenAI tool as if it could appear on a billboard in Times Square.

Privileged Automation is Possible—Offline

Not all automation requires cloud access or third-party servers.

TheFormTool® PRO and Doxserá® are the only leading document automation products confirming a privileged, confidential environment for concerned law firms. Used by thousands of law firms across North America and around the world, they offer robust au-

© TheFormTool, LLC

tomation while operating. Unlike their cloud-based competitors—including those that have added generative AI integration—they operate:

- 100% offline
- With zero external communication
- Fully under the user's control

There are no silent data leaks. No backdoors. No default storage in someone else's data-center.

All work product stays where the lawyer puts it: on a local machine, firm network, or virtual private server.

Recommendations for Bars and Ethics Boards

Bar associations and ethics committees can take clear, nonpartisan steps to protect client privilege:

- Issue formal guidance on the risks of cloud-based GenAI platforms.
- Encourage or require disclosure to clients if such tools are used.
- Support offline or local-first tools for privileged work.
- Provide CLE programming to educate members on AI-related ethics.
- Develop model disclaimers and engagement letters to address AI usage.
- Review vendor practices to determine whether cloud AI or remote processing is used in document automation platforms marketed to the legal industry.

These actions can help the legal profession adapt to powerful new technologies without sacrificing its most essential obligations.

TheFormTool® PRO and Doxserá ® are the only major document automation programs that operate entirely offline, with no internet connection required and no background communication of any kind. This guarantees that client data never leaves your system.

ABA Rule 1.6

More about security

Significant Firms in the Document Assembly and Automation Space

More about Doxserá

More about TheFormTool PRO

TheFormTool LLC

www.theformtool.com

info@theformtool.com

© TheFormTool, LLC