

Understanding the Risks of Uploading Client Information to Generative AI Platforms

[Nicholas Daniel Seger](#)

Jan 16, 2024  7 min read



Practice Management

Technology

Ethics

Summary

- At the core of the attorney-client relationship lie your ethical and legal obligations to maintain confidential client information and protect your client's privileged information.
- You must determine the risks involved in uploading confidential client information to resources such as Grammarly, ChatGPT, and Lexis+ AI and educate yourself on the potential risks of using these platforms so you may take steps reasonably calculated to maintain client confidentiality.
- Best practices include refraining from uploading confidential data to AI platforms, researching technology providers thoroughly, obtaining client consent, and educating clients on the benefits and risks of AI.
- By making yourself an expert on new technology, you not only fulfill your ethical duties and mitigate the risks of disclosing confidential client information but also make yourself a valuable asset to your organization.






iStock.com/ridvan celik

Lawyers owe sacrosanct [ethical and legal obligations](#) to their clients. Among the most important of these include the duty to maintain client confidentiality, protect privileged client communications, and apprise the client of the risks and benefits of proposed legal strategies. A lawyer's inadvertent breach of these duties may irreparably harm the client, stain the lawyer's reputation, and subject the lawyer to ethical complaints and malpractice actions.



The recent substantial improvements in artificial intelligence present [a challenge for lawyers](#) but also provide an opportunity for new lawyers who lack the experience and knowledge of their more distinguished colleagues. Although this technology is new, it's not unique. By considering the ethical rules and looking to past examples of how the legal profession has adapted to and coped with new technologies, you can provide yourself and your clients with a path forward that allows for the use of these valuable resources wh^o  understanding and mitigating the risks involved with any new technology.

Understanding Your Ethical and Legal Responsibilities

At the core of the attorney-client relationship lie your ethical and legal obligations to [maintain confidential client information and protect your client's privileged information](#). You must also reasonably inform your client of the manner of the representation and potential risks involved in your representation. Because the attorney-client bond also presents a contractual relationship, you must consider your client's reasonable expectations when you enter that contract to ensure that you fulfill your end of the representation agreement.

Uploading and relying on artificial intelligence implicates all of these responsibilities. You must first determine the risks involved in uploading confidential client information to resources such as Grammarly, ChatGPT, Lexis+ AI, and the like. You also must educate yourself on the potential risks of using these platforms so you may take steps reasonably calculated to maintain client confidentiality. Specifically, you should carefully read the terms and conditions of service and privacy statements and research the company. This will allow you to determine whether the service provider shares inputted information with third parties, intends to sell the information provided, and the extent to which you and your client may reasonably expect that client information will remain confidential if provided to the platform.

For example, [ChatGPT recently incurred a data breach](#) that potentially exposed many users' data, including names, payment information, passwords, and chat histories. This shows the vulnerabilities that new companies and new technologies often present. Any successful rollout of something new and exciting will elicit a wave of attacks from those determined to steal valuable data.

Uploading Privileged Information

Currently, there remains a plausible argument that uploading confidential client information or privileged client information would destroy confidentiality and privilege.

[AI, including ChatGPT] can record a single user's notes on any topic and then summarize that information or search for more details. But if those notes include sensitive data—an organization's intellectual property or sensitive customer information, for instance—it enters the [platform's] library. The user no longer has control over the information.

["ChatGPT Confirms Data Breach, Raising Security Concerns,"](#) *Security Intelligence*, May 2, 2023.



Uploading client information to an AI platform potentially exposes the information to an external third party who has not, depending on the privacy agreement and policies, explicitly agreed to maintain your client's confidentiality. We know that most AI platforms use all inputted data to improve their algorithms and analytic abilities. Therefore, at least theoretically, you're allowing third parties to use your client's information in a way that doesn't benefit your client and could potentially benefit your client's adversaries. There also remains a remote risk that humans may search a platform's database and uncover your client's confidential or privileged information. Grammarly, for example, states that it may, under certain limited circumstances, have its employees review any data you input into its system.

With the proliferation of [generative AI platforms](#) such as ChatGPT, Google Bard, Grammarly, Lexis+ AI, and others, you should expect a wide range of privacy protections and controls provided by the offering company. You should never assume that a company has agreed to keep the information confidential or private, has robust security against data breaches, or will not use or sell the information you provide unless you have thoroughly researched the issue with the provider.

Best Practices for Use of Confidential Information and AI

Lawyers are notoriously slow adopters of new technologies, and for good reason. The client protections described above and the repercussions for inadvertent disclosure present a high risk for a population of risk-averse professionals in the legal field. However, you should not shy away from implementing AI. In fact, the model rules of professional conduct require you to keep abreast of this new technology, understand it, and implement it effectively for your client.

At this time, and with the information we currently have on the common generative AI platforms, it's smarter and safer to abstain from uploading confidential client information or privileged documents to these platforms. Instead, consider rewriting or summarizing your questions or arguments in a generic way that could not reasonably be traced back to your client. Take an approach similar to one you would take if you were speaking with another lawyer not involved with your case to obtain advice on an ethical matter. As the model rules state, this is permissible under certain circumstances, so long as you don't present information in a way that would make your client or your client's confidential or privileged information identifiable in any way. As always, the most prudent course of action is to educate yourself fully on the risks of use and to obtain informed client consent before you use AI to assist you in representing your clients.



Researching the Technology

Thoroughly look into the company's history, privacy statements, policies, procedures, and any other relevant information you can find before placing your client's information in jeopardy. This may include in-person discussions with company representatives before you implement the technology. You should track and log your diligence and self-education in this realm. In the worst-case scenario, you must at least show that you took all reasonable steps to ensure your client's confidentiality when using any new platform. While this may at first seem burdensome, the time you spend on these tasks will improve your competency and use of AI and provide you with peace of mind and defensibility in any future potential objections to your use of AI technology.


Don't Forgo Client Consent

Any time a new technology presents a risk, you should strongly consider obtaining your client's informed consent to use that technology before doing so. If you thoroughly research the technology you plan to use and advise your clients of the benefits and risks, then you provide yourself and your client with the best scenario to determine, collaboratively, how to best proceed with the client representation. This practice aligns with how you should always communicate with clients, regardless of the issue presented: after undertaking your due diligence and research, you should always seek to fully apprise your clients of any substantial risk in your representation strategies.

Contractual Obligations to Clients

Recall that your representation of a client is, at its core, a contractual one. If your client does not expect you to use generative AI in your representation, your client may become upset and feel that you breached your client's reasonable expectations in the representation. Some people still want a human to do all of the work. Until generative AI becomes more widely known and accepted, this provides another strong reason to obtain informed client consent before using this technology to represent clients.

A Broader Perspective of AI

Looking back to the adoption of cloud-based storage and the risks that this technology imposed may provide us with perspective. In the beginning, lawyers, courts, and clients grappled with the permissibility of its use due to the uncertainty regarding the security of the platforms available. Over time, lawyers and courts have researched the providers available, weighed the risks of breach, taken efforts to educate themselves on the best practices of using cloud-based storage, and have since effectively incorporated it into ' practice. Importantly, clients now understand and appreciate the effectiveness of cloud 

based storage and expect lawyers to implement it to save resources on their behalf. Clients understand the risks involved and how to work with their lawyers to mitigate those risks.

You should similarly seek to educate your clients on the use of generative AI, the benefits you expect it to provide, and the associated risks. Then, your clients may make an informed decision on whether the potential cost of a data breach or loss of confidential information is worth the benefit in savings that generative AI promises to bring. In the coming years, we will all become comfortable using different forms of AI to further our practice of law, and this level of detail may become unnecessary. However, at this time of transition and relative uncertainty, you should err on the side of caution and proceed mindfully.

Looking to the Future

As a new lawyer, you must embrace new technology and expect to adapt to it continuously throughout your career. Constantly educating yourself on the technology, best practices for its use, and how it works will give you a distinct advantage over lawyers who choose not to embrace it early on. By making yourself an expert on new technology, you not only fulfill your ethical duties and mitigate the risks of disclosing confidential client information but also make yourself a valuable asset to your organization.

Author



Nicholas Daniel Seger

Nicholas Seger is an Assistant Professor of Academic Success at the University of Dayton School of Law. He teaches courses focused on foundational law school skills, as well as Business Organizations and Emerging Legal...

