GC AI↲

Untitled chat

Carolyn

When an attorney uses CHAT GPT or CLAWD to research a legal issue, are those communications with those AI platforms considered subject to attorney-client privilege or work product doctrine?

GC AI

2 September 2025 at 13:44 GMT-4

GC AI used think tool

Carolyn, this is an interesting question at the intersection of legal doctrine and new technology.

For attorney-client privilege:

- Communications with AI platforms like ChatGPT or CLAWD generally wouldn't qualify for attorney-client privilege on their own, as the AI isn't your client.
- However, if you're using these tools to prepare advice for a specific client, the research process could potentially be considered part of privileged work.
- The key issue is that privilege typically requires confidential communications between attorney and client - the AI platform represents a third party, which could break the privilege chain.

For work product doctrine:

- This has stronger potential protection. Materials prepared by an attorney in anticipation of litigation receive protection regardless of whether a client is involved.
- Your AI research queries and the resulting outputs could qualify as attorney work product if they reflect your mental impressions, conclusions, or legal theories for a case.
- Courts would likely analyze whether the AI interactions were created because of the prospect of litigation.

Practical considerations:

- Confidentiality is crucial - using public AI platforms with data retention policies creates risk.
- Some platforms now offer specific legal versions with enhanced confidentiality protections.
- Document your use of AI tools as part of your legal research process.
- Be mindful that inputting confidential client information into these platforms could potentially waive privilege.

The law is still developing in this area, with courts only beginning to address these questions.

Carolyn

Okay, so just to clarify, let's say that I do a research project for a client. Say the client is getting divorced and has questions about child support. If I research that issue on Google or ChatGPT, you're telling me that research is not privileged and somebody could get it in Discovery?

GC AI

2 September 2025 at 13:46 GMT-4

GC AI used think tool

Carolyn, let me clarify this important distinction:

The research process itself (your searches, queries, notes) would likely be protected under the work product doctrine if you're doing that research specifically for a client's case. This protection applies to materials prepared by an attorney in anticipation of litigation or representation, regardless of the tools used.

However, there are some important nuances:

For Google searches:

- The fact that you performed certain searches isn't typically stored in a way that's accessible to opposing counsel
- Your search history is private to your account/device
- The work product doctrine would protect your research notes and process

For ChatGPT:

- The key risk is that you're sharing potentially sensitive information with a third-party platform
- The conversations are stored on OpenAI's servers
- While the work product doctrine should still apply, using a third-party service creates a potential argument for waiver

The final advice you give your client about child support would absolutely be protected by attorney-client privilege.

The bottom line is that your research materials should be protected as work product, but using third-party platforms does create some additional risk compared to using legal research platforms specifically designed for attorneys with confidentiality protections built in.

Carolyn

Cite the sources you have that say that when information is stored on a third-party platform, it loses attorney-client protection. I mean, why wouldn't that be true of cloud-based practice management systems?

GC AI

2 September 2025 at 13:48 GMT-4

GC AI used think tool

GC AI performed research for the following queries: "attorney client privilege third party platforms AI ethics opinions", "cloud based practice management attorney client privilege waiver", "reasonable expectation of confidentiality third party services legal privilege", "work product doctrine AI research tools legal ethics"

GC AI used think tool

You're right to challenge me on this, Carolyn. My statement about third-party platforms was overly broad and lacked important nuance.

The key distinction isn't simply whether information is stored on a third-party platform, but rather:

1. Whether the third party is considered an agent of the attorney
2. Whether adequate confidentiality protections are in place
3. Whether there's a reasonable expectation of privacy
4. The specific terms of service of the platform
5. How the platform uses, retains, or shares data

Cloud-based practice management systems designed specifically for legal use typically have confidentiality agreements and security measures that help preserve privilege. As noted in ABA Formal Opinion 512 (July 2024), lawyers must "ensure that the GenAI system is configured to preserve the confidentiality and security of information, that the obligation is enforceable, and that the lawyer will be notified in the event of a breach." [1]

The Florida Bar has noted that "the use of an in-house generative AI program rather than one that requires data to be stored by an outside, third-party generative AI program may mitigate confidentiality concerns." [2]

The critical issue is whether engaging with a platform constitutes disclosure to a third party that breaks the privilege chain. According to a recent JD Supra article, "If a client provides privileged details to a platform managed by an entity not directly engaged by the law firm for legal support, courts may determine that privilege has been forfeited." [3]

For work product protection specifically, a recent case (Tremblay v. OpenAI) suggests that attorneys' interactions with AI tools may be protected, particularly if they contain the attorney's "mental impressions and opinions." [4]

So the better analysis is that privilege depends on the specific platform, its terms of service, confidentiality protections, and how it's used - not simply whether it's third-party hosted.

Carolyn

Can you check the terms of service for Anthropic Clawed and see if it provides that level of third-party protection from disclosure? Claude

GC AI

2 September 2025 at 13:51 GMT-4

GC AI used think tool

GC AI performed research for the following queries: "Anthropic Claude terms of service data privacy confidentiality", "Anthropic Claude legal users attorney client privilege protection", "Anthropic Claude data retention policy how inputs are used", "Anthropic Claude vs ChatGPT privacy terms comparison legal users"

Carolyn

Can you retry the response?

GC AI

2 September 2025 at 13:54 GMT-4

Of course. Based on my research, here is a breakdown of Anthropic Claude's terms and how they relate to third-party protection and disclosure.

The critical factor is the distinction between Anthropic's *consumer* products and its *commercial* products.

Consumer Claude (Free, Pro, and Max)

Using the consumer versions of Claude for privileged information carries significant risk.

- **Data for Training:** As of August 2025, Anthropic asks consumer users to choose whether their data can be used to train its models. [5] While you can opt out, the default setting is to opt-in.
- **Data Retention:** If you allow your data to be used for training, Anthropic extends the data retention period to five years. [6] If you opt out, the standard 30-day retention period applies, but conversations flagged for trust and safety reviews can be kept for up to two years. [7] [8]
- **Third-Party Risk:** Because consumer data can be used for training (unless you opt out) and is subject to review, it is being disclosed to a third party (Anthropic) in a manner that does not align with the requirements for maintaining attorney-client privilege.

Commercial Claude (Claude for Work, API)

The commercial versions of Claude offer much stronger protections that are more suitable for legal work.

- **No Training on User Data:** The policy updates allowing data use for training explicitly **do not** apply to commercial services like Claude for Work or the API. [9] Anthropic states, "We will not use your Inputs or Outputs to train our models." [10]
- **Data Deletion:** For API users, inputs and outputs are deleted within 30 days, unless a specific zero-data retention agreement is in place. [11] For Claude for Work, you control your conversation history and can delete it, and it will be removed from back-end systems within 30 days. [12]
- **Contractual Protections:** Anthropic offers a Data Processing Addendum (DPA) and is willing to enter into Business Associate Agreements (BAA) for commercial customers, providing contractual assurances about data handling and confidentiality. [13]

Conclusion:

The commercial versions of Anthropic Claude, particularly when governed by a DPA or a zero-data retention agreement, appear to provide the necessary level of third-party protection to safeguard privileged information. The consumer versions do not.

Citations

[^1]: * Ensure that the GenAI system is configured to preserve the confidentiality and security of information, that the obligation is enforceable, and that the lawyer will be notified in the event of a breach or service of process regarding production of client information;

- Investigate the GenAI system's reliability, security measures, and policies, including limitations on the system's liability;

Source: https://www.frantzward.com/privilege-considerations-when-using-generative-artificial-intelligence-in-legal-practice

[^2]: The Florida Bar noted that the use of an in-house generative AI program rather than one that requires data to be stored by an outside, third-party generative AI program may mitigate confidentiality concerns. However, a proposed formal opinion issued by the North Carolina State Bar cautions that even an in-house program that seems more secure because it is maintained and run on local servers could be more vulnerable to attack if it lacks security features used by larger companies with greater cybersecurity capabilities. Consequently, an attorney who plans to use an in-house generative AI program should consult information technology and cybersecurity professionals about how best to protect client information stored on a local server.

Source: https://info.wealthcounsel.com/blog/ethical-implications-of-generative-ai

[^3]: A critical legal issue is whether engaging an AI platform constitutes disclosure to a third party. Attorney-client privilege generally applies only to confidential communications between the lawyer and client, or their necessary agents. If a client provides privileged details to a platform managed by an entity not directly engaged by the law firm for legal support, courts may determine that privilege has been forfeited.

Source: https://www.jdsupra.com/legalnews/client-beware-the-utilization-of-7208312

[^4]: Judge Araceli Martinez-Olguin, writing for the District Court, found that "ChatGPT account settings and negative test results" constitute opinion work product, rather than fact work product. *Tremblay v. OpenAI, Inc.*, No. 23-cv-3223, at 3 (N.D. Cal. Aug. 8, 2024). The court reasoned that "the ChatGPT prompts were queries crafted by counsel and contain counsel's mental impressions and opinions about how to interrogate ChatGPT, in an effort to vindicate Plaintiffs' copyrights against the alleged infringements." *Id*. (citing *Republic of Ecuador v. Mackay*, 742 F.3d 860, 869 n.3 (9th Cir. 2014)). Since the requests involved opinion work product, a higher standard for establishing waiver applied, and OpenAI, the requesting party, failed to satisfy that standard. *Id*. at 4 & n.3 (citing *United States v. Sanmina Corp.*, 968 F.3d 1107, 1119 (9th Cir. 2020)).

Source: https://www.redgravellp.com/publication/uncharted-waters-work-product-protections-for-attorneys-use-of-generative-ai

[^5]: Today, we're rolling out updates to our Consumer Terms and Privacy Policy that will help us deliver even more capable, useful AI models. We're now giving users the choice to allow their data to be used to improve Claude and strengthen our safeguards against harmful usage like scams and abuse. Adjusting your preferences is easy and can be done at any time.

Source: https://www.anthropic.com/news/updates-to-our-consumer-terms

[^6]: We are also extending data retention to five years, if you allow us to use your data for model training. This updated retention length will only apply to new or resumed chats and coding sessions, and will allow us to better support model development and safety improvements. If you delete a conversation with Claude it will not be used for future model training. If you do not choose to provide your data for model training, you'll continue with our existing 30-day data retention period.

Source: https://www.anthropic.com/news/updates-to-our-consumer-terms

[^7]: That is a massive update. Previously, users of Anthropic's consumer products were told that their prompts and conversation outputs would be automatically deleted from Anthropic's back end within 30 days "unless legally or policy-required to keep them longer" or their input was flagged as violating its policies, in which case a user's inputs and outputs might be retained for up to two years.

Source: https://techcrunch.com/2025/08/28/anthropic-users-face-a-new-choice-opt-out-or-share-your-data-for-ai-training

[^8]: We retain inputs and outputs for up to 2 years and trust and safety classification scores for up to 7 years if you submit a prompt that is flagged by our trust and safety classifiers as violating our Usage Policy.

Feedback Data

Source: https://privacy.anthropic.com/en/articles/10023548-how-long-do-you-store-my-data

[^9]: These updates apply to users on our Claude Free, Pro, and Max plans, including when they use Claude Code from accounts associated with those plans. They do **not** apply to services under our Commercial Terms, including Claude for Work, Claude Gov, Claude for Education, or API use, including via third parties such as Amazon Bedrock and Google Cloud's Vertex AI.

Source: https://www.anthropic.com/news/updates-to-our-consumer-terms

[^10]: "We will not use your Inputs or Outputs to train our models, unless: (1) your conversations are flagged for Trust & Safety review (in which case we may use or analyze them to improve our ability to detect and enforce our Usage Policy , including training models for use by our Trust and Safety team, consistent with Anthropic's safety mission), or (2) you've explicitly reported the materials to us (for example via our feedback mechanisms), or (3) by otherwise explicitly opting in to training." — from https://support.anthropic.com/en/articles/7996885-how-do-you-use-personal-data-in-model-training

Source: https://medium.com/@michael_79773/ai-assistant-privacy-what-claude-chatgpt-and-gemini-users-should-now-7d3f5cae9e5d

[^11]: For Anthropic API users, we automatically delete inputs and outputs on our backend within 30 days of receipt or generation, except when you and we have agreed otherwise (e.g. zero data retention agreement), if we need to retain them for longer to enforce our Usage Policy (UP)

Source: https://privacy.anthropic.com/en/articles/7996866-how-long-do-you-store-my-organization-s-data

[^12]: You control your conversations and can delete your chats anytime from your dashboard. When you delete a conversation it's:

- Removed from your chat history immediately
- Deleted from our back-end storage systems within 30 days

Usage Policy Violations

Source: https://privacy.anthropic.com/en/articles/7996866-how-long-do-you-store-my-organization-s-data

[^13]: Where can I learn more about Anthropic's Privacy practices? Business Associate Agreements (BAA) for Commercial Customers What Certifications has Anthropic obtained? What is Anthropic's policy for handling governmental requests for user information? Why am I receiving an 'Output blocked by content filtering policy' error? I think a user is infringing my copyright or other intellectual property. How do I report it? How do I view and sign your Data Processing Addendum (DPA)? Why am I receiving an 'Output blocked by content filtering policy' error? Updates to our Acceptable Use Policy (now "Usage Policy"), Consumer Terms of Service, and Privacy Policy Consumer Terms of Service Updates Terms of Service Updates Official Anthropic marketing email addresses Reporting, Blocking, and Removing Content from Claude Does Anthropic crawl data from the web, and how can site owners block the crawler? Online Safety Contacts Claude 4 Invite Sweepstakes Official Rules Designated Point of Contact for Users in the EU

Source: https://support.anthropic.com/en/collections/4078534-privacy-and-legal