Stanford Law Review Online

Volume 79 September 2026

ESSAY

AI Privilege and the Legal Services Crisis

Andrea Roth & Rebecca Wexler*

Introduction

Recently, San Francisco public defenders were so overburdened that they risked jail for contempt rather than take on more cases.[1] Wyoming and New Mexico public defenders have done the same, while other states have been sued for underfunded, ineffective public defender systems.[2] Meanwhile, some people accused of low-level crimes have no lawyer whatsoever, making critical decisions about pleading guilty or trial strategies on their own, and being subject to pretrial detention, significant fines, and collateral consequences like deportation and sex offender registration.[3] Even outside the criminal system, low-income people face evictions, family separations, deportations, and more with inadequate legal assistance.

This Essay explores a key but misunderstood doctrinal question related to this nationwide crisis: Could exchanges between laypeople and Artificial

* Andrea Roth is the Professor of Law and Barry Tarlow Chancellor's Chair in Criminal Justice, University of California, Berkeley, School of Law. Rebecca Wexler is the Alfred W. Bressler Professor of Law, Columbia Law School. The authors thank Brandon Garrett, Jerome Greco, and Edward J. Imwinkelried for critically helpful comments; Meghan Mitchell and Lauren Pelosi for excellent research assistance; and the editors of the *Stanford Law Review Online* for their insightful editorial guidance.

1. *Appeals Court Again Blocks Contempt Sanction Against SF Public Defender*, DAILY J. (Apr. 13, 2026), https://perma.cc/49Z9-WNUX.

2. *See* Clair McFarland, *Wyoming Public Defender Held in Contempt Fights Charge, Quits*, COWBOY ST. DAILY (Jan. 23, 2025), https://perma.cc/TFB7-SZ3J; Debra Cassens Weiss, *Public Defender Is Found in Contempt for Refusing Cases; DA Asks State Supreme Court to Intervene*, ABA J. (Dec. 1, 2016, 2:16 PM CST), https://perma.cc/N8BB-N96L; *Indigent Defense*, ACLU, https://perma.cc/F373-YZRW (archived July 17, 2026) (noting pending cases involving suits against public defender agencies).

3. Indeed, by some estimates, over half of federal criminal defendants are forced to proceed pro se. *See* Erica J. Hashimoto, *The Price of Misdemeanor Representation*, 49 WM. & MARY L. REV. 461, 489-90 & n.128 (2007). *See generally* Andrea Roth, *The Embarrassing Sixth Amendment*, 112 CALIF. L. REV. 55, 70 (2024) (discussing the limits of the right to counsel and the consequences of misdemeanor prosecutions).

Intelligence (AI) chatbots like Claude or ChatGPT, seeking legal advice, ever be protected by privilege law, such as the attorney-client privilege and work-product doctrine? The question is timely, as clients and pro se litigants increasingly turn to chatbots for legal research and advice and as the government has repeatedly accessed or tried to access such exchanges to use them as evidence against a litigant, and argued that no privilege applies.[4] At least one court has agreed with the government. A federal judge recently ruled in *United States v. Heppner* (S.D.N.Y.)[5] that a criminal defendant's legal queries to Claude—which the government found while executing a warrant to search his computer, and which the defendant claimed he was planning to share with his attorney—were fair game to introduce at trial. The judge in *Heppner* rejected the defendant's attorney-client privilege claims out of hand, reasoning simply that Claude is not an attorney.[6]

Legal commentary on the issue has been split. Some would, as the judge in *Heppner*, categorically reject attorney-client privilege claims for litigant-chatbot exchanges, arguing that the privilege extends solely to communications directly with, or at least directed by, a lawyer.[7] And Sam Altman, CEO of OpenAI, has publicly opined that exchanges should be, but are not, legally protected, and has suggested a new "AI privilege."[8] Those who argue that existing privilege law protects at least some litigant-chatbot exchanges contend primarily that Claude is simply a "tool," like Google Docs or a notepad, rather than a person.[9]

4. *See, e.g.*, Opposition to Motion to Quash at 1, United States v. Kim, 2026 WL 1785995 (S.D.N.Y. June 22, 2026) (No. 25 Cr. 359), ECF No. 55 (seeking to uphold a warrant on OpenAI for the defendant's ChatGPT prompts).

5. 820 F. Supp. 3d 292 (S.D.N.Y. 2026).

6. *See id.* at 296. The judge in *Heppner* reasoned that lack of confidentiality and a non-legal purpose also negated privilege, but that Claude's non-attorney status was sufficient to doom the claim all on its own. *Id.* at 296-97.

7. *See, e.g.*, Ira P. Robbins, *Against an AI Privilege*, HARV. J.L. & TECH. DIG. (Nov. 7, 2025), https://perma.cc/NCJ6-SHUB (describing the doctrine established in United States v. Kovel, 296 F.2d 918 (2d Cir. 1961), as covering exchanges with third parties "assisting the lawyer," "enabl[ing] the lawyer," and "used under counsel's direction," apparently excluding exchanges that assist, enable, and/or are directed by the client); Jonah E. Perlin, *No, Generative AI Didn't Just Kill the Attorney-Client Privilege*, BLOOMBERG L. (Aug. 12, 2025, 4:30 AM EDT), https://perma.cc/JG99-U8NT ("All that matters from the attorney-client privilege perspective is that no lawyer is present in the communication. . . . [Individuals] should avoid using those tools themselves and instead hire lawyers who can use the tools . . . .").

8. Sam Altman (@sama), X (June 5, 2025, at 12:33 AM PDT), https://perma.cc/SB34-DT8P ("[W]e have been thinking recently about the need for something like 'AI privilege'; this really accelerates the need to have the conversation. imo [sic] talking to an AI should be like talking to a lawyer or a doctor.").

9. *See* Elizabeth X. Guo, *United States v. Heppner*, HARV. L. REV. BLOG (Mar. 23, 2026), https://perma.cc/H68B-FFH3 (acknowledging that attorney-directed exchanges with a non-attorney "person" would still qualify for the privilege under *Kovel*, but arguing that AI is just a "tool" and, thus, its confidential use to facilitate future communications

footnote continued on next page

But attorney-client privilege doctrine already protects many confidential exchanges with non-attorneys so long as they are *necessary to facilitate legal services from the client's lawyer.* Moreover, what commentators on both sides seem to have forgotten is that this necessity test has never turned on whether the lawyer or the client directed the exchange.[10] At a minimum, at least some litigant-chatbot exchanges could presumably meet this test, regardless of how one resolves thorny metaphysical questions about whether a chatbot is more akin to a tool or a person.

Further, *Heppner*'s flat rejection of the defendant's work-product argument was also incorrect. Contrary to the judge's and some commentators' assumptions, work-product doctrine does not apply merely to materials created by attorneys.[11] Rather, in both civil and criminal cases, work-product protections explicitly apply—at least under the federal rules of procedure—to materials created by the parties themselves.[12] Granted, a party's own work-product protection, at least in civil cases, is more limited; unlike the near-absolute protection against discovery given to attorneys' mental impressions, a party's work-product protection in civil cases can be overcome by a showing of sufficient need, at least where the party is represented by counsel rather than appearing pro se.[13] But a party's exchanges with AI should potentially enjoy significant work-product protection either way.

To be sure, the attorney-client privilege and the work-product doctrine impose real costs by shielding relevant information from factfinders. Some exchanges, such as ChatGPT prompts by a suspect in recent Florida shootings asking how best to conceal the crime,[14] should undoubtedly remain discoverable. But the way to acknowledge these costs is not to reject privilege claims out of hand just because they involve AI rather than an attorney. That

with a lawyer is akin to a client's notepad and would be protected without even triggering a *Kovel*-like inquiry into necessity); *cf.* Bridget McCormack & Shlomo Klapper, *A Judge Mistakes the Claude Chatbot for a Person*, WALL. ST. J. (Apr. 6, 2026, 12:58 PM ET) (arguing that exchanges with Claude do not "waive" the privilege because Claude is not a person, appearing to treat the *Heppner* decision as one related to waiver). We explain our disagreement with this waiver argument further in Part I.D.

10. *Cf.* Guo, *supra* note 9 (favoring privilege but presuming that the *Kovel* doctrine applies solely to communications "between a client and an *attorney's* non-attorney agent," thus omitting client-initiated consultations) (emphasis added); Robbins, *supra* note 7 (disfavoring privilege but presuming the same); Perlin, *supra* note 7 (same).

11. *Cf.* Robbins, *supra* note 7 (describing the work-product doctrine as protecting solely "an *attorney*'s mental impressions and trial preparations" and ordinary rules as applying "[w]here AI assists *counsel*" (emphasis added)).

12. *See infra* Part II.

13. *Compare* FED. R. CIV. P. 26(b)(3)(A) (allowing discovery of parties' work product upon a showing of substantial need), *with* FED. R. CIV. P. 26(b)(3)(B) (providing more absolute protection for the "mental impressions, conclusions, opinions, or legal theories of a party's attorney or other representative concerning the litigation"). *See also infra* Part II.

14. *See* Mark Osborne, *College Students' Killings Latest Case to Rely on ChatGPT as Evidence*, CBS NEWS (Apr. 29, 2026, 8:17 AM EDT), https://perma.cc/4D6Q-SA29.

approach contradicts existing law and may well be undesirable as a policy matter, given the potential promise of AI in mitigating the legal services crisis. In any event, courts should faithfully apply existing privilege law to these exchanges and see how the chips fall. If, after doing so, they conclude that reform is necessary to expand or retract the privilege in the age of AI, the power to change current law is well within courts' and legislatures' reach but should be exercised explicitly.

In the two sections below, we explain how current attorney-client privilege and work-product law, properly understood, will protect many, even if not all, litigant-chatbot exchanges. In Part I, we explain how existing attorney-client privilege doctrine already incorporates a necessity test for communications with non-attorneys that, we contend, should apply to AI exchanges as well. In Part II, we explain how work-product doctrine already applies to non-attorney litigants by rule and should presumptively apply to their AI exchanges. We conclude by considering the potential need for doctrinal reform and implications for the lawyering crisis.

I. Attorney-Client Privilege and Chatbots: Apply the Necessity Test

In this section, we explain the necessity test for protecting communications involving non-attorneys and how that test aligns with the purpose of the attorney-client privilege. We then lay out a normative case for applying the necessity test to litigant-chatbot exchanges.

A. Overview of the Attorney-Client Privilege

The attorney-client privilege protects confidential communications between clients and attorneys made for purposes of facilitating legal services. To be protected, an exchange must be a *communication* (not, say, merely conduct witnessed by an attorney); must be treated by the client as *confidential*; must generally be between an *attorney* and a *client*, although in some circumstances the privilege includes communications to agents of both; and must be for the purpose of facilitating legal services from the attorney (not, say, merely an exchange about non-legal matters with a friend who happens to be an attorney). In the federal system and some states, the privilege is entirely a creature of common law; in other states, the privilege is statutory. But these basic elements of the privilege apply broadly throughout the country.[15]

The purpose of the privilege is to encourage fair and frank communications by clients to their attorneys, ensuring that attorneys can give

15. *See, e.g.*, DAVID A. SKLANSKY & ANDREA L. ROTH, EVIDENCE: CASES, COMMENTARY, AND PROBLEMS 657-68 (6th ed. 2025) (noting the privilege's common-law provenance and its elements, citing case law around the country).

the best legal advice possible.[16] In turn, ensuring attorneys can provide the best legal advice helps clients understand the law and thereby avoid illegal activity, and levels the playing field between legally sophisticated and unsophisticated clients. The privilege also has costs, most notably that it keeps relevant information from factfinders and law enforcement. One justificatory theory is that, without the privilege, clients would likely not make unfavorable statements to begin with.[17] Another theory concedes the costs but argues that they are justified by dignitary benefits; specifically, the privilege preserves the client's dignity by ensuring a safe space for someone facing legal battles to talk to at least one person who is on their side.[18]

B. The Existing Necessity Test for Communications Involving Non-Attorneys

Inevitably, both clients and their attorneys must sometimes communicate, or share information, with others to facilitate legal services. For example, an attorney might need to consult with an expert in another discipline, sharing client information,[19] or a client might need to speak with that same expert or consultant at the attorney's direction.[20] An attorney might also need to research a topic on Westlaw relevant to the representation and, in the process, be compelled to reveal information that implicitly discloses a client's communications to Westlaw's owner, the Thomson Reuters corporation.[21] Moreover, to help facilitate a future conversation with a lawyer, a client might need to share information with another person. For example, the client might

16. *See* Swidler & Berlin v. United States, 524 U.S. 399, 403, 411 (1998) (explaining the purpose of the privilege and holding that it survives the client's death).

17. *See, e.g.*, Ronald J. Allen, Mark F. Grady, Daniel D. Polsby & Michael S. Yashko, *A Positive Theory of the Attorney-Client Privilege and the Work Product Doctrine*, 19 J. LEGAL STUD. 359, 374, 380 (1990) (discussing the behavioral incentives framework in which the privilege is justified if it applies to disclosures that would not have been made absent the privilege).

18. *See, e.g.*, Edward J. Imwinkelried, Essay, *The New Wigmore: An Essay on Rethinking the Foundation of Evidentiary Privileges*, 83 B.U. L. REV. 315, 333-37 (2003) (advancing a "humanistic" theory that the privilege is necessary to protect personhood because it creates private enclaves that ensure a trusting relationship with a consulting expert).

19. *See, e.g.*, United States v. Kovel, 296 F.2d 918, 920-21 (2d Cir. 1961); Alexander v. FBI, 192 F.R.D. 12, 16 (D.D.C. 2000); *see also* 8 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2301 (John T. McNaughton ed., rev. ed. 1961) ("It has never been questioned that the privilege protects communications to the attorney's clerks, and his other agents . . . for rendering his services." (emphasis omitted)).

20. *See, e.g.*, *Kovel*, 296 F.2d at 922 ("[T]he presence of the accountant, *whether hired by the lawyer or by the client* . . . ought not destroy the privilege . . . ." (emphasis added)).

21. *See, e.g.*, Calogero v. Shows, Cali & Walsh, No. 18-6709, 2021 WL 8572978, at *3 (E.D. La. Dec. 23, 2021) ("Generally, research undertaken by an attorney to respond to a client's request falls within the reaches of [attorney-client] privilege."); Nguyen v. Excel Corp., 197 F.3d 200, 206 (5th Cir. 1999) ("[T]he research undertaken by an attorney to respond to a client's request also falls within the reaches of the [attorney-client] privilege.").

need to speak to an interpreter or other non-attorney to figure out how to explain relevant details to an attorney.[22] Or clients may need to conduct research in a library,[23] and, in the process, be compelled to reveal information to a librarian or digital service provider that implicitly reveals the contents of communications they are preparing to share with their lawyer.

Existing doctrine rightly holds that attorney-client privilege sometimes applies in these types of circumstances, despite the disclosures to non-attorneys. The privilege's application does not turn on the presence or absence of an attorney at any given moment in the communication pipeline. Instead, application of the privilege turns on *whether the disclosure was necessary to facilitate legal services from an attorney*.[24]

Admittedly, case law is somewhat ambiguous about precisely how courts should determine which disclosures qualify. The leading precedent, *United States v. Kovel* from Judge Friendly of the Second Circuit, describes the test as "necessary, or at least highly useful,"[25] though some cases use the word

22. *See, e.g.*, Farahmand v. Jamshidi, No. CIV.A.04-542, 2005 WL 331601, at *3 (D.D.C. Feb. 11, 2005) (noting that there are circumstances in which "a communication by a client to his attorney by any form of agency employed or set in motion *by the client* is within the privilege" (quoting Mileski v. Locker, 178 N.Y.S.2d 911, 915-16 (Sup. Ct. 1958))).

23. *Cf.* Bounds v. Smith, 430 U.S. 817, 828 (1977), *abrogated by* Lewis v. Casey, 518 U.S. 343 (1996) (recognizing the needs of pro se incarcerated persons to access legal research materials).

24. *See, e.g.*, Sampedro v. Silver Point Cap., L.P., 818 F. App'x 14, 18-19 (2d Cir. 2020) (holding that attorney-client privilege attached to communications that included "a third-party consulting firm" because the firm was "*essential* in interpreting large quantities of data" (emphasis added)); In re Bieter Co., 16 F.3d 929, 939 (8th Cir. 1994) (considering whether disclosures to a non-attorney third-party contractor were "*necessary*" (emphasis added)); Diversified Indus., Inc. v. Meredith, 572 F.2d 596, 605 (8th Cir. 1977) (Henley, J., concurring in part and dissenting in part on the hearing en banc) (discussing how confidentiality is maintained despite disclosures to "those *reasonably necessary* for the transmission of the communication" (emphasis added)); *Kovel,* 296 F.2d at 922 (finding that the third-party must be "*necessary, or at least highly useful*, for the effective consultation between the client and the lawyer which the privilege is designed to permit" (emphasis added)); Don v. Singer, No. 105584-06, 2008 WL 2229743, at *5 (N.Y. Sup. Ct. 2008) (noting that the party asserting the agency exception must show that "disclosure to the third party was *necessary* for the client to obtain informed legal advice" (emphasis added)); Allied Irish Banks, PLC v. Bank of Am., N.A., 240 F.R.D. 96, 104 (S.D.N.Y. 2007) ("[W]here the third party's presence is merely 'useful' but not '*necessary*,' the privilege is lost." (emphasis added) (quoting Nat'l Educ. Training Grp., Inc. v. Skillsoft Corp., No. M8-85, 1999 WL 378337, at *5 (S.D.N.Y. June 10, 1991))); *Farahmand*, 2005 WL 331601, at *3 ("The reasonable *necessity* exception[] allow[s] clients to communicate through intermediaries under certain circumstances . . . ." (emphasis added)); *Mileski*, 178 N.Y.S.2d at 916 ("[C]ommunications to any person whose intervention is *necessary* to secure and facilitate the communication between attorney and client are privileged, as communications through an interpreter, a messenger, or any other intermediary." (emphasis added)).

25. *Kovel,* 296 F.2d at 922. This test has been quoted widely. *See* Lluberes v. Uncommon Prods., LLC, 663 F.3d 6, 24 (1st Cir. 2011); Cavallaro v. United States, 284 F.3d 236, 247 (1st Cir. 2002); SEC v. Navellier & Assocs., No. 17-11633, 2019 WL 285957, at *2 (D. Mass. Jan. 22, 2019); Glob. Textile All. v. TDI Worldwide, LLC, 847 S.E.2d 30, 35 (N.C.

footnote continued on next page

"essential."[26] The First Circuit has elaborated "that the 'necessity' element means more than just useful and convenient. The involvement of the third party must be nearly indispensable or serve some specialized purpose . . . . Mere convenience is not sufficient."[27] Nor is the fact that a communication merely "significantly assisted" the provision of legal services or later "prove[d] important[.]"[28]

What is crystal clear is that the mere presence of a non-attorney is not a dealbreaker. Of particular note, prior commentators seem to have missed that the necessity test applies even when the necessary non-attorney agent is chosen by the client and not the lawyer.[29] The existing doctrine is thus well-positioned to address client-initiated chatbot exchanges.

C. Applying the Necessity Test to Exchanges with AI Chatbots

Courts can and should apply the existing necessity test to litigant-chatbot exchanges. At least some chatbot exchanges would surely be protected under this test. A client might show, for example, that the client used the chatbot to prepare for a meeting by organizing information for the attorney or translating an idea into words an attorney would understand, and that the client reasonably viewed the exchange as necessary to help the client receive services from the lawyer. A client might also reasonably believe that their lawyer alone is unable to do sufficient research or analysis to provide adequate legal services. This concern is not hypothetical, as evidenced by litigation around the country over ineffective provision of indigent defense services. While a client would not be able to expect protection for every instance in

---

2020); *see also* Dunn v. Patriarch Partners, LLC, 672 B.R. 587, 591 (Bankr. D. Del. 2025) (collecting cases that extend *Kovel* beyond accountants to other "third part[y] agents who provide specialized assistance *necessary* to the issuance, comprehension, and execution of counsel's legal advice" (emphasis added)).

26. *Sampedro,* 818 F. App'x at 19.

27. *Cavallaro,* 284 F.3d at 249 (quoting EDNA SELAN EPSTEIN, THE ATTORNEY-CLIENT PRIVILEGE AND THE WORK-PRODUCT DOCTRINE 187 (4th ed. 2001)).

28. United States v. Ackert, 169 F.3d 136, 139 (2d Cir. 1999).

29. *See, e.g., Kovel,* 296 F.2d at 921-22 ("[W]e can see no significant difference between a case where the attorney sends a client speaking a foreign language to an interpreter . . . [and a case] where someone to perform that same function has been *brought along by the client*." (emphasis added)); *Sampedro,* 818 F. App'x at 18-19 (noting that the privilege attached despite the involvement of "a third-party consulting firm retained *by [the client]*" (emphasis added)); Grand Jury Procs. Under Seal v. United States, 947 F.2d 1188, 1191 (4th Cir. 1991) ("[C]ommunications *between the client and his agent* made for the purpose of facilitating the rendition of legal services would be covered by the privilege." (emphasis added)); *Farahmand,* 2005 WL 331601, at *1 (concluding that privilege attached to the client's Farsi notes made to assist in communicating with his attorney, despite the fact that when the client discussed the notes with his attorney, his son-in law was "present and serving as an *ad hoc* interpreter"); *Mileski,* 178 N.Y.S.2d at 915-16 ("[A] communication by a client to his attorney by any form of agency employed or set in motion *by the client* is within the privilege." (emphasis added)).

which they ask a chatbot for legal advice or a "second opinion" after hearing from their lawyer, they should have the opportunity to present evidence to meet the necessity test, including, for example, supporting affidavits from their attorney.[30]

To be sure, canonical applications of the necessity rule thus far have been in circumstances where the attorney lacked *expertise* to communicate with a client, such as knowledge of a foreign language or accounting techniques, whereas the need with overburdened public defenders is more likely to stem from lack of time and resources. But there is no bright-line distinction between these two scenarios. Even in the canonical cases, attorneys with infinite time and resources could have developed the necessary expertise themselves. Hence, the core precedents can all be framed as recognizing that an attorney's lack of time and resources can lead to a gap in knowledge necessary to advise a client.

Of course, another way of interpreting existing doctrine to apply privilege to a client's chatbot exchanges is to treat them as a mere conduit tool, like Google Docs or Google Slides, which courts generally accept in privileged communications without requiring a showing of necessity.[31] But AI chatbots are not mere conduit tools; clients use them not simply to organize or memorialize their own thoughts but also to acquire new expertise by interacting with a consultant.[32] Given the necessity test that applies under current law to clients' communications with human experts, it would seem odd if a client could enjoy near-absolute secrecy in chatbot exchanges based solely on showing a reasonable expectation of confidentiality and a purpose of obtaining legal advice. Entirely gratuitous chatbot prompts would be covered, undermining the truth-seeking process while adding little to the quality of legal services. On the other hand, it might not make sense to treat chatbots exactly like human interlocutors (such as an accountant or interpreter) either, given that they have (at least as of this writing) more limited agency in certain respects. Perhaps they, like Westlaw and other nonhuman "consultants," fall on a spectrum between Google Docs and human experts, justifying secrecy based on a lesser showing than necessity. At a minimum, though, chatbot exchanges should be eligible for privilege protection if they satisfy the necessity test that applies to non-attorney humans.

Courts applying the necessity test to chatbot exchanges should also bear in mind that—contrary to the assumptions of some courts and commentators—an

30. *Cf.* Motion to Quash at 4, United States v. Kim, 2026 WL 1785995 (S.D.N.Y. June 15, 2026) (No. 25 Cr. 359), ECF No. 52 (representing to the trial court that the client's ChatGPT prompts were "in connection with communications with counsel" and for the purpose of facilitating legal services).

31. *See* Guo, *supra* note 9 (citing cases where attorney-client privilege covered a client's Google Docs and Google Slides notes taken in preparation for a communication with their attorney and observing that "courts seem to treat that tool's non-attorney status as immaterial to the privilege analysis").

32. Thank you to Edward J. Imwinkelried for helpfully articulating this distinction.

AI chatbot's use of prompts for training purposes should not necessarily destroy the privilege. Yes, a client must treat a communication as confidential for it to be privileged and waives the privilege by later treating a privileged communication as non-confidential.[33] For example, someone who places notes where everyone can see them, or who shares privileged information with a trusted friend who then betrays them, has likely destroyed the privilege. But the test is whether the client takes reasonable steps to ensure confidentiality, not whether the secrecy of the interaction is, in fact, perfectly preserved.[34] Thus, a client's communications to someone posing as a licensed attorney are protected so long as the client reasonably believed the person was an attorney.[35] The law does not burden clients with investigating their lawyer's bar discipline history, whether their private residence is being wiretapped, or the technical fine print of an online service. Moreover, even if a chatbot uses prompts for external training purposes (meaning that the prompts could in theory be incorporated into future answers to other users), specific inculpatory details linked to an identified client are unlikely to make their way to third parties.

Of course, applying the necessity rule to litigant-chatbot exchanges will be heavily fact-specific,[36] and the doctrine will inevitably evolve through common-law iteration. This is a good thing. Iteration will enable courts to carefully balance the potential good of AI assistance with concerns that overexpansion of privilege might unduly impede truth-seeking or incentivize attempts to launder otherwise-unprotected communications through AI systems.[37] We do not purport to know exactly where the line should be drawn.

---

33. *See* CHRISTOPHER B. MUELLER, LAIRD C. KIRKPATRICK & LIESA L. RICHTER, EVIDENCE § 5.29 (6th ed. 2018) (explaining the confidentiality element of privilege as well as waiver of an already privileged communication based on later disclosure).

34. Similarly, most state ethics opinions permit lawyers to use cloud services so long as they take "reasonable steps to ensure that sensitive client information remains confidential and safeguarded." ALASKA BAR ASS'N, ETHICS OPINION 2014-3, at 1 (2014), https://perma.cc/ZJ4W-JT3F (archived July 17, 2026); *see also* Daniel W. Linna Jr. & Wendy J. Muchman, *Ethical Obligations to Protect Client Data When Building Artificial Intelligence Tools: Wigmore Meets AI*, PROF. LAW., Fall 2020, at 27, 30, https://perma.cc/TH9T-YUS6.

35. *See, e.g.*, United States v. Boffa, 513 F. Supp. 517, 523 (D. Del. 1981) (explaining why privilege still applies where client reasonably but mistakenly believes the communication is to a licensed attorney).

36. Notably, applying a necessity rule to *Heppner* itself might not have resulted in a different outcome. If the issue had been properly litigated under the correct legal rule, the record might have been more robust and could have indicated that Mr. Heppner's Claude exchanges were not actually necessary for the provision of legal services in his case.

37. Applying the necessity test will also create an opportunity for judicial balancing beyond the purpose prong of the privilege, as to which "[u]ser-AI interactions are heterogeneous, and after-the-fact purpose parsing at internet scale [could] be unworkable." *See* Robbins, *supra* note 7.

Those concerned about overprotection should remember that proponents retain the burden of proof, and that exceptions to the privilege, such as for exchanges enabling a crime or fraud, would still apply. But it should be beyond dispute that focusing on whether the communication was made directly to, or directed by, an attorney, or on whether a chatbot is a "tool" or a "person," gets it wrong, both in terms of what the law is and what it should be.

D. Conflating Privilege with Waiver

A final analytical misstep in the discourse about privilege and chatbots—this one by critics of *Heppner*—merits comment. Some commentary appears to assume that *Heppner* was wrong, and that chatbot exchanges are protected, because the client intended the chatbot disclosures to be confidential and treated them as such, and thus did not "waive" the privilege.[38] But the ruling in *Heppner* was not that the client's exchanges with Claude "waived" the privilege with respect to the client's original disclosures to his attorneys, or his attorneys' disclosures to him. Instead, *Heppner*'s ruling was that the exchanges themselves were not privileged to begin with.[39]

Although *Heppner*'s conclusion on privilege was wrong, it was right to focus on whether the chatbot exchanges themselves were privileged, not on whether those exchanges "waived" the privilege with respect to earlier disclosures. To see why, imagine a client who tells his attorney "I robbed the bank," and then the following night writes in his diary, "I robbed the bank. I also told my lawyer this." The original communication to the lawyer, if made in confidence and to facilitate legal services, is privileged. And it is true that the client's diary entry does not waive that privilege and allow the opposing party to subpoena the lawyer. But the diary entry itself is not privileged; if the government finds it when executing a search warrant in the client's house, the entry—at least the part confessing to the crime—is fair game. In the same respect, a chatbot exchange in which a client confesses a crime is not itself protected by the privilege simply because the client may have revealed the same information to an attorney previously.

38. *See, e.g.*, McCormack & Klapper, *supra* note 9. Note that only the client, not the attorney, can waive the privilege. If an attorney shares the client's information in a way that is not authorized by the client and that allows a third party to access the information, the privilege generally still applies. *See, e.g.*, Carmody v. Bd. of Trs. of Univ. of Ill., 893 F.3d 397, 406 (7th Cir. 2018) (deeming privilege not waived by an inadvertent email disclosure by the attorney). Still, an attorney's use of ChatGPT for research can be ethical and even encouraged, assuming it is done responsibly and is not likely to expose the client's information to those who would use it against the client. *Cf.* Calogero v. Shows, Cali & Walsh, LLP, No. 18-6709, 2021 WL 8572978, at *3 (E.D. La. Dec. 23, 2021) (opining that legal research done by an attorney on behalf of a client is within the scope of privilege).

39. *See* United States v. Heppner, 820 F. Supp. 3d 292, 296-98 (S.D.N.Y. 2026).

However, if the entry (or chatbot exchange) *does* satisfy the necessity rule, it is and should be protected by privilege of its own right. In short, clients like Mr. Heppner cannot rely on waiver doctrine to show their chatbot exchanges are protected. But they also need not rely on waiver doctrine because they may, depending on the facts, have a strong argument that the exchanges themselves are privileged.

II. Work-Product Doctrine and Chatbots: Litigants Count Too

The *Heppner* court also erroneously rejected the claim that a client's chatbot exchanges may be protected by the "work product" doctrine. The opinion incorrectly assumed that the doctrine applies only to materials created by attorneys. In fact, many chatbot exchanges, including with litigants who have no attorney at all, are likely protected as work product.

The work-product doctrine protects from discovery certain materials prepared by parties and their agents in anticipation of litigation. The purpose of the doctrine is to promote efficiency and fairness "in the giving of legal advice and in the preparation of cases for trial," on the assumption that the inability of litigants to prepare for trial "with a certain degree of privacy, free from unnecessary intrusion by opposing parties and their counsel," would be "demoralizing."[40]

The doctrine is codified in the federal rules of civil and criminal procedure, which both explicitly protect material created by the parties themselves, not merely by their attorneys. In civil cases, the text of the rules protects material "prepared in anticipation of litigation or for trial *by or for another party* or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent)," unless the requesting party shows a "substantial need for the materials" and inability to access their equivalent otherwise "without undue hardship."[41] It is true that in civil cases, an even greater level of absolute protection is afforded to "the mental impressions, conclusions, opinions, or legal theories *of a party's attorney or other representative* concerning the litigation."[42] But even this near-absolute level of additional protection has been extended by some courts to include not just attorneys but pro se

40. Hickman v. Taylor, 329 U.S. 495, 510-11 (1947).

41. FED. R. CIV. P. 26(b)(3)(A) (emphasis added). Notwithstanding the plain text of Rule 26, the Fifth Circuit has held that materials prepared by a client are categorically ineligible for work-product protection. *See* United States v. Davis, 636 F.2d 1028, 1039-40 (5th Cir. 1981) (citing United States v. Nobles, 422 U.S. 225, 237-38 (1975)); *see also* United States v. Jimenez, 265 F. Supp. 3d 1348, 1353-54 (S.D. Ala. 2017) (ruling that notes the defendant emailed to himself about topics he wanted to discuss with his attorneys were not protected by work-product privilege because "the law of [the Eleventh] Circuit is that materials prepared by a client are not protected by the work product doctrine").

42. FED. R. CIV. P. 26(b)(3)(B) (emphasis added).

litigants.[43] Indeed, two courts have recently ruled that a pro se civil litigant's exchanges with a chatbot were non-discoverable work product.[44] Meanwhile, the federal criminal rules by their text contain no such caveats, providing blanket protection against discovery of "reports, memoranda, or other documents *made by the defendant, or the defendant's attorney or agent,* during the case's investigation or defense."[45]

Given the text of the rules, it is not self-evident why work-product protection should exclude litigant-AI exchanges. Of course, like attorney-client privilege, work-product doctrine carries risk in terms of excluding relevant information from factfinders. But as with attorney-client privilege, the proponent of work-product protection carries the burden of showing the doctrine applies, and some chatbot exchanges might not qualify. In Mr. Heppner's case, for example, although his prompts to Claude were surely "documents made by the defendant . . . during the case's investigation or defense," and Claude's answers presumably revealed the gist of those prompts, the government could still execute its search warrant, and in arguing for access to the exchanges, might have shown a substantial need.[46] Yet neither side in

43. *See, e.g.,* Brockmeier v. Solano Cnty. Sheriff's Dep't, No. CIV S-05-2090, 2010 WL 148179, at *6 (E.D. Cal. Jan. 12, 2010) ("However, plaintiff will not be ordered at this time to produce any notes prepared in anticipation of litigation which reveal her mental impressions and/or legal strategies."); Nielsen v. Soc'y of New York Hosp., No. 87 CIV. 8526, 1988 WL 100197, at *2 (S.D.N.Y. Sept. 22, 1988) ("If plaintiff were represented by counsel, his attorney's notes in similar circumstances would not be subject to production. A plaintiff appearing *pro se* is entitled to no less protection."). *But see* Jennifer A. Gundlach & Zeus Smith, *Expanding the Federal Work Product Doctrine to Unrepresented Litigants*, 30 GEO. J. ON POVERTY L. & POL'Y 49, 65-66 (2022) (noting a court split on this issue).

44. Warner v. Gilbarco, 820 F. Supp. 3d 629, 636 (E.D. Mich. 2026); Morgan v. V2X, Inc., No. 25-CV-01991, 2026 WL 864223, at *3-4 (D. Colo. Mar. 30, 2026). In *Morgan*, the ruling on work product was arguably dictum, given that the defendant's sole request of the pro se plaintiff was disclosure of the name of the AI program the plaintiff used to confirm whether the program's confidentiality features sufficiently protected the defendant's own information. *Id.* at 1.

45. FED. R. CRIM. P. 16(b)(2)(A) (emphasis added). Presumably for this reason, government access to work product in criminal cases is typically through warrant or grand jury subpoena rather than discovery, and courts have applied a "substantial need" test to grand jury subpoenas. *See, e.g.,* In re Grand Jury Subpoena Dated July 6, 2005, 510 F.3d 180, 184-86 (2d Cir. 2007).

46. Privilege law does not immunize materials from seizure pursuant to a valid warrant. *See, e.g.,* Google LLC v. United States, No. 23-67, 2025 WL 4958336, at *5 (D.D.C. Feb. 25, 2025) (collecting cases to support the proposition that courts have "uniformly rejected [privilege-based] pre-execution challenges to [Stored Communications Act] warrants by the customers or subscribers whose information is sought"); Order at 1-2, United States v. Kim, 2026 WL 1785995 (S.D.N.Y. June 22, 2026) (No. 25 Cr. 00359), ECF No. 56 (denying the defendant's privilege-based challenge to a warrant seeking chatbot exchanges). Privilege can, however, limit the scope of a post-seizure search. *See, e.g.,* United States v. Gallego, No. CR-18-01537-001, 2018 WL 4257967, at *1, *3 (D. Ariz. Sept. 6, 2018) (appointing a special master to determine which seized documents were covered by attorney-client or work-product privilege); In re Grand Jury Subpoenas

footnote continued on next page

Heppner could fully and fairly litigate these issues, because the court never got past the assumption that solely attorneys are protected. Moreover, the doctrine does not protect materials created for ordinary business purposes or when there is a mere speculative possibility of being prosecuted or being involved in a lawsuit someday. The point here is not that chatbot exchanges will always be protected as work product, but that the doctrine's application should be based on correct application of existing law and evolve in an iterative process as courts realize the stakes on both sides.

One of the key stakes in terms of work product is, again, access to justice. Civil litigants have no general constitutional right to an attorney, even if they face jail time,[47] and criminal defendants have no such right unless they are actually sentenced to jail time.[48] While using AI to prepare one's case comes with great risk given AI's well-known fallibilities, AI could be crucially beneficial to someone who is facing a criminal prosecution or civil suit without any legal representation.[49] Imagine a low-income lay criminal defendant having to assess the legality and benefits of a plea offer, file motions, seek discovery, talk to witnesses, pick a jury, write an opening statement, and prepare cross-examinations by himself. To allow the government to discover his strategic conversations with AI before trial could be devastating to his defense and would not have happened had those same prompts to AI been made by a lawyer.

Dated Dec. 10, 1987, 926 F.2d 847, 858-59 (9th Cir. 1991) (deeming seized documents unprivileged but recognizing the need for *in camera* review to determine this); In re Sealed Search Warrant, 11 F.4th 1235, 1240, 1249-50, 1252 (11th Cir. 2021) (affirming district court's imposition of filter protocol on seized documents to determine if any were covered by attorney-client or work-product privilege); *see also* Anna Dincher, Comment, *How to Fix DOJ Privilege Teams*, 2 U. CHI. BUS. L. REV. 429, 430-31 (2023) (noting that the government acknowledges that seized documents are still covered by privilege law and must be filtered by government "privilege teams").

47. Turner v. Rogers, 564 U.S. 431, 448 (2011). Indeed, there is a presumption against a constitutional right to counsel in parental termination cases. Lassiter v. Dep't of Soc. Servs., 452 U.S. 18, 25-31 (1981). Nor is there a statutory right to appointed counsel in immigration cases. *See* 8 U.S.C. § 1362 (establishing a right only to retained counsel not at government expense).

48. Scott v. Illinois, 440 U.S. 367, 369 (1979) (holding that no constitutional right to appointed counsel exists even for a jury-demandable offense where no jail time was actually imposed). Many states, and the federal government, also have no statutory right to appointed counsel where no jail time is imposed. *See* Roth, *supra* note 3, at 69-70.

49. The issue of whether AI has helped or hindered courts' review of pro se pleadings is a separate one. *See* Mattathias Schwartz & Zach Montague, *Artificial Intelligence Floods Court Dockets with Home-Brewed Lawsuits*, N.Y. TIMES (last updated May 28, 2026), https://perma.cc/L6C6-ABZ5. Litigants' use of AI to write pleadings will surely continue regardless of how privilege law is applied to inculpatory details and mental impressions in underlying prompts.

Conclusion

Existing attorney-client privilege and work-product protections for party-created documents already offer potential protection of litigant-AI chatbot exchanges when properly applied. These doctrines have evolved over time to address the very hard line-drawing problem of balancing the costs and benefits of privilege law, and they can address those same line-drawing problems as applied to litigant-AI exchanges. At the least, these existing doctrines are the right place for courts to start when considering privilege claims for AI chatbots. If it turns out that application of these doctrines to AI exchanges raises unforeseen, unique challenges, courts and legislatures would be free to modify the scope of protection to meet those challenges, based on "reason and experience."[50] Indeed, any federal district judge could create a novel AI privilege upon concluding it "promotes sufficiently important interests to outweigh the need for probative evidence,"[51] and many state judges could as well. But those powers to alter existing law should be exercised explicitly, after clearly considering how current doctrine would apply.

On a final preemptive note, our optimism regarding the promise of AI to ameliorate certain aspects of the legal services crisis should not be taken as a belief that a chatbot is a substitute for a lawyer, even an overtaxed or underprepared one. But if there are cases where a client can show that an exchange was "necessary, or at least highly useful"[52] to, or "serve[d] some specialized purpose"[53] for a lawyer's representation, or a pro se litigant can show that an exchange helped them prepare to represent themselves, then we should not let our concerns about AI lead to ignoring existing law and rejecting privilege claims out of hand. As anyone who has relied on AI can attest, we should not delegate the world's problems to a chatbot to solve. But neither should we irrationally reject AI's potential where it could help solve intractable problems if used responsibly. Indeed, where it helps achieve justice, AI can—perhaps counterintuitively—make the system more humane.

50. FED. R. EVID. 501. For example, some courts have begun expanding work product protection to "business strategy" in transactional work, rather than merely materials strictly in anticipation of litigation. *See generally* Edward J. Imwinkelried, *The Narrow Evidentiary Question of Whether Litigators' Work Product Immunity Should Be Extended to Business Strategy Documents and the Broader Policy Question of Whether the Work of Litigators Differs in Kind from the Work of Transactional Attorneys*, 19 OHIO ST. BUS. L.J. 39 (2024).

51. Jaffee v. Redmond, 518 U.S. 1, 8-12 (1996) (quoting Trammel v. United States, 445 U.S. 40, 51 (1980)) (recognizing that privilege law is a creature of common law).

52. *See supra* note 25 and accompanying text.

53. Cavallaro v. United States, 284 F.3d 236, 249 (1st Cir. 2002) (quoting EPSTEIN, *supra* note 27, at 187).