BRIEFING FOR GENERAL COUNSEL · NOVEMBER 2026

Privilege and AI

Attorney-client privilege, work product, and what happens to your AI chats

Kimball Parker

Law current through November 9, 2026 · For education; not advice on any specific matter

AGENDA

Five questions, then what to do about them

I	**Privilege and work product**	Elements, waiver, and the two different waiver rules
II	**Privilege inside a business**	Upjohn, the primary-purpose test, Kovel agents
III	**Is AI use privileged?**	Heppner, Warner, Morgan, and the 2026 split
IV	**Ephemeral and deleted AI chats**	Rule 37(e), Epic v. Google, In re OpenAI
V	**Vetting AI tools**	Contract terms and technical controls
→	**Recommendations**	Eleven practices and a one-page checklist

THE BOTTOM LINE

AI doesn’t create privilege, and it rarely destroys it on its own

PRIVILEGE

A client’s own consumer-AI chats are not privileged

Privileged facts typed into the tool can be waived. United States v. Heppner (S.D.N.Y. 2026)

WORK PRODUCT

AI-assisted litigation prep often stays protected

An AI provider isn’t an adversary. Six of eight rulings, incl. Fontainebleau (Oct. 2026)

PRESERVATION

AI chats are ESI: preserve them like email

Deleted chats were ordered kept. In re OpenAI (2025); Epic v. Google (2023)

THE DECISIVE FACTS Who directed the AI use · the tool’s terms · whether it was prepared because of litigation

Privilege and work product are two shields with different waiver rules

	Attorney-client privilege	Work product
Protects	Confidential communications for legal advice	Materials prepared because of litigation
Created by	Client, lawyer, necessary agents (Kovel)	The party or any representative
Waived by	Disclosure to any third party	Disclosure to an adversary, or that makes it likely
Overcome by	Nothing: absolute once established	Substantial need (fact work product only)
Sharing with a tool	**Usually waives**	**Usually not a waiver**

Hickman v. Taylor (1947); Fed. R. Civ. P. 26(b)(3); Fed. R. Evid. 502; United States v. Deloitte, 610 F.3d 129 (D.C. Cir. 2010)

II · PRIVILEGE INSIDE A BUSINESS

Inside a company, the corporation is the client, and it controls the privilege

Any employee can be inside the privilege

If the employee communicates at counsel's direction, for legal advice, about their own duties. Upjohn v. United States (1981)

Management holds and can waive it

Including over a former executive's objection. CFTC v. Weintraub (1985). Give Upjohn warnings in interviews.

Agents can sit inside it

Kovel agents who help counsel give advice, and contractors who are the functional equivalent of employees

WHERE THE RULE DIFFERS

Illinois still uses the narrower control-group test.

EU competition law gives no privilege to in-house lawyers (Akzo Nobel, 2010).

Assume in-house AI workflows get less protection abroad.

II · THE PRIMARY-PURPOSE TEST

Dual-purpose communications are where in-house privilege breaks down

MORE PROTECTIVE

“One of the significant purposes”

In re Kellogg Brown & Root, 756 F.3d 754 (D.C. Cir. 2014). Investigations required by regulation can still be privileged.

LESS PROTECTIVE

“The primary purpose”

In re Grand Jury, 23 F.4th 1088 (9th Cir. 2021). Certiorari dismissed in 2023; the split remains.

> A “privileged” label is evidence of intent, not proof of privilege. Broad distribution and business content defeat it.

II · WHERE AI ENTERS

AI multiplies the in-house privilege risks that already exist

Embedded assistants

Copilot-style tools mix legal and business content in widely shared records. The dual-purpose problem, at scale.

AI meeting summaries

A summary of a call with counsel, auto-sent to every attendee, can defeat need-to-know.

Employee self-help

Pasting counsel's advice into a personal chatbot to "make sense of it" can waive the company's privilege.

Represented executives

The company controls its AI tool, and consumer tools fail Heppner. No safe option.

II · WHAT PEER COMPANIES ARE DOING

Peers are layering policy, contracts, and oversight

Company	What it requires
Lenovo	No public AI tools for work; only licensed, approved tools
Demotech	No confidential data in consumer AI; enterprise tools only with IT and compliance approval
SitusAMC	Vendors need Legal's approval before putting privileged material into AI
UBS	Outside counsel need in-house approval to use AI, and must disclose it in bills
Zscaler	No training on its data; lawyers must review AI-generated deliverables
BNY	Multi-board AI governance, with Legal reviewing AI uses

41% of legal departments have never audited for shadow AI (ACC)

38% of enterprises have comprehensive AI-use policies (ISACA)

III · THE LEADING DECISION

Heppner: a client's own consumer-AI chats are not privileged

S.D.N.Y. · FEB 17, 2026 · RAKOFF, J.

A fraud target used consumer Claude to outline his defense after a subpoena. Agents seized ~31 AI documents. Counsel hadn't directed the use.

THE OPENING

Had counsel directed it, Claude "might arguably" act as the lawyer's agent under Kovel.

Not a lawyer
Two non-lawyers discussing legal issues isn't privileged.

Not confidential
The privacy policy allowed training and disclosure to authorities.

Not for legal advice from a lawyer
Sending outputs to counsel later doesn't help.

No work product
Not prepared at counsel's behest; didn't reflect counsel's strategy.

Waiver of what he typed in
Privileged facts shared with the tool were waived.

III · THE RULINGS SO FAR

Six of eight rulings protected AI work; both losses involved represented parties acting alone



III · HOW COURTS REASONED

The deciding question is who used the AI, and at whose direction

Case	Who used the AI	Result	Key reasoning
Tremblay v. OpenAI	Counsel, testing prompts	**Protected**	Attorney prompts are opinion work product
Warner v. Gilbarco	Pro se plaintiff	**Protected**	Waiver needs an adversary; AI is a tool
U.S. v. Heppner	Represented defendant, alone	**Not protected**	No lawyer, no confidentiality, no direction
Morgan v. V2X	Pro se plaintiff	**Protected**	Vendor storage isn't waiver; name the tool
Tate Group	Party principal	**Protected**	Texas rule; rejected Heppner's reasoning
Assini v. Hayward	Pro se defendant	**Protected**	Quashed account-wide subpoena to OpenAI
Shealy v. Seaside	Partner, at party's request	**Not protected**	Partner not the party's representative
Fontainebleau	Party, no counsel direction	**Protected**	Rejected Heppner's rule; log each item

III · ENTERPRISE TOOLS

Enterprise terms fix confidentiality, not the other two elements

CAN BE SATISFIED

Made in confidence

No-training, no-disclosure terms answer Heppner's privacy-policy problem.

STILL FAILS

With a lawyer

An AI isn't an attorney, whatever the contract says.

STILL FAILS

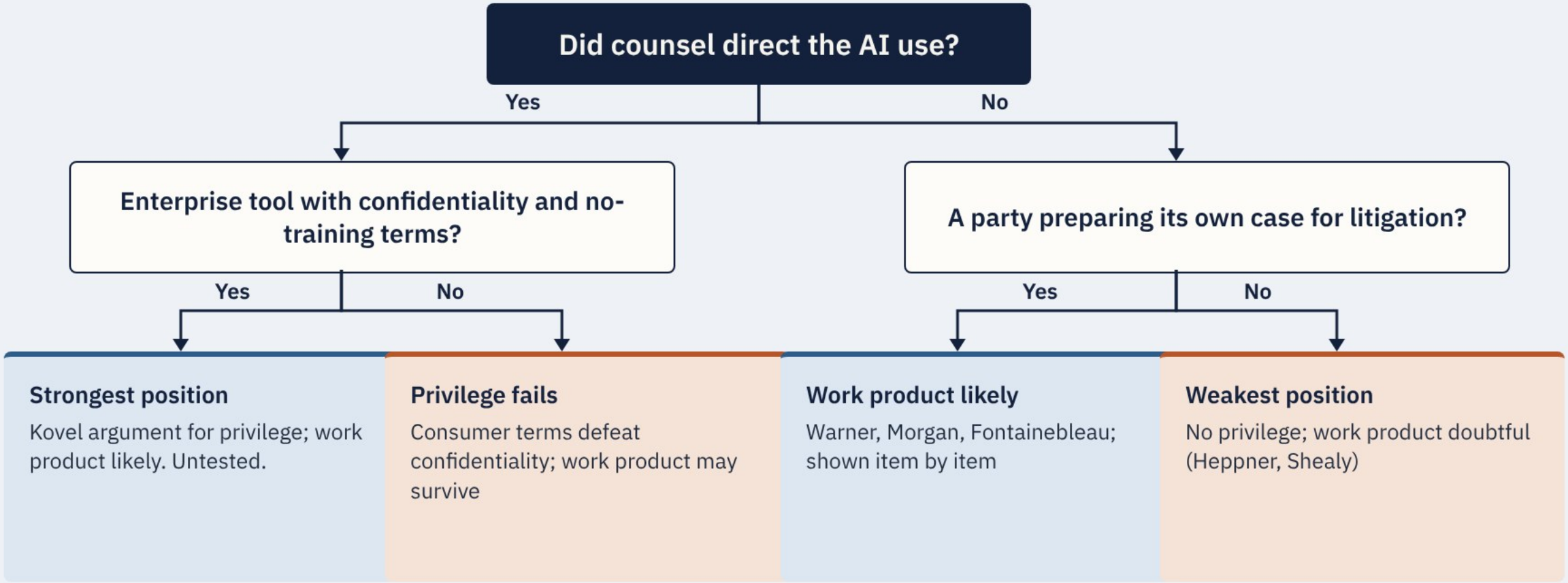
For legal advice

The tool disclaims giving legal advice; the government proved it by asking.

THE FIX Counsel's direction supplies the missing elements. No court has yet tested it.

III · IS THIS AI USE PROTECTED?

Start with who directed the AI use



IV · EPHEMERAL AND DELETED AI CHATS

Deleting AI chats is lawful until the duty to preserve attaches

BEFORE THE DUTY

Routine deletion under a written, consistently applied policy

TRIGGER

Litigation reasonably anticipated

AFTER THE DUTY

Prompts, outputs, and logs are ESI. Preserve them like email.

Rule 37(e)(1): prejudice

Measures “no greater than necessary” to cure the harm

Rule 37(e)(2): intent to deprive

Adverse-inference instruction, dismissal, or default judgment

Deleting records to impede an investigation can also be obstruction: 18 U.S.C. §§ 1512(c), 1519.

IV · THE EPHEMERAL-MESSAGING PRECEDENT

Ephemeral settings have already drawn sanctions

2020

WeRide v. Huang

Adopted an auto-deleting chat app after the duty attached. Terminating sanctions.

2023

Epic v. Google

“History off” by default; employees chose what to keep. Fees, then an adverse-inference instruction.

2024

DOJ and FTC

Preservation letters and subpoenas now name ephemeral tools. Failure may mean obstruction charges.

Temporary Chat and auto-delete are the new “history off.”

IV · IN RE OPENAI (S.D.N.Y.)

“Deleted” isn’t gone when your AI vendor is under a court order

May 2025

Preservation order covers logs that “would otherwise be deleted,” including chats users deleted. Enterprise and Edu carved out.

Sept–Oct 2025

Ongoing obligation ends. Logs already kept, and flagged accounts, stay preserved.

Nov 2025

Court orders a 20-million-chat de-identified sample produced.

Jan 2026

Affirmed: users lack substantial privacy interests in chats given to the platform.

LESSON

Contract terms decided whose chats were kept. Consumer accounts were swept in; enterprise accounts weren’t.

ALSO: FONTAINEBLEAU (2026)

The plaintiff subpoenaed all four AI vendors the defendant used.

IV · RETENTION RISK

Risk turns on timing and on who controls deletion

	Before the duty attaches	After the duty attaches
Deletion set by policy, enforced by IT	LOW RISK · DEFENSIBLE Routine deletion on a documented, consistently applied schedule	LOW RISK · REQUIRED IT suspends auto-delete and Temporary Chat; hold names AI tools
Deletion left to users, ad hoc	ELEVATED RISK Looks selective, and invites an inference of bad faith if litigation follows	HIGH RISK · SANCTIONABLE Epic, WeRide: fees, adverse inference, terminating sanctions

V · VETTING AI TOOLS: CONTRACTS

“No training” isn’t the whole contract

Term	What to check
Secondary use	Whether de-identified data can still be used, e.g. for benchmarking
Retention	Platform, model provider, logs, and backups can each differ
Platform vs. model	A platform can keep data even when its model provider keeps none
Access	Human review and every subprocessor that touches the data
Legal process	Notice to you if someone subpoenas the vendor
Model changes	New models and features can carry different data terms
Liability	Caps that limit what a confidentiality promise is worth

V · VETTING AI TOOLS: TECHNICAL CONTROLS

Software can block uploads, but it can’t recognize privilege

Coach and block at upload

Netskope (embecta), Nightfall (Unit21, UserTesting)

Browser isolation

Zscaler (CNA): AI allowed, but no uploads or copy-paste

Microsoft Purview for Copilot

Gaps for files uploaded into prompts; fix in preview Jan. 2027

THREE CAUTIONS

Tools detect sensitive data, not legal advice.

Guardrails inside a tool may still log the original.

DLP forensics can save the very memo it blocked.

> Test it: paste, type, upload, search a restricted folder, then inspect the logs.

RECOMMENDATIONS

You can’t change the doctrine. You can control the facts courts weigh.

- Who directs
- Which tool
- Which terms
- What purpose
- How long logs live

RECOMMENDATIONS

Control the facts in three places: tools, workflows, and retention

Tools and terms

1. Approve AI tools by contract: no training, confidentiality, set retention
2. Block consumer AI for legal work with DLP or browser controls
3. Hold outside counsel to the same AI standards

Workflows

1. Have counsel direct legal AI work in writing (Kovel-style)
2. Use separate, access-limited legal workspaces per matter
3. Send AI summaries of legal calls to counsel only
4. Train employees on the Heppner trap

Retention and litigation

1. Put AI logs in the records schedule
2. Make holds AI-aware, and have IT enforce them
3. Add AI clauses and Rule 502(d) orders to protective orders
4. Prepare for AI-log requests, including vendor subpoenas
5. Have an incident plan for leaked privileged material

CHECKLIST

An AI privilege checklist for in-house teams

- [ ] Approved tools vetted by contract; terms on file
- [ ] Consumer AI restricted for legal work
- [ ] Written counsel direction for privileged AI work
- [ ] Access-controlled legal AI workspaces per matter
- [ ] AI summaries of legal calls routed to counsel
- [ ] Employee training on personal and consumer AI
- [ ] Outside-counsel guidelines updated for AI
- [ ] Records schedule covers prompts, outputs, uploads, agent logs
- [ ] Hold template names AI tools; IT runbook suspends auto-delete
- [ ] Control tests run; incident plan for leaks
- [ ] Protective-order AI clauses and Rule 502(d) language ready
- [ ] Privilege-log approach for AI materials agreed

DEVELOPMENTS TO WATCH

Six open questions will shape this law in 2027

Appellate review

No circuit has ruled, and Fontainebleau openly rejected Heppner's rule.

Counsel-directed AI

Untested: does Kovel cover an AI tool counsel directs?

Enterprise terms

Do no-training contracts preserve privilege? Not yet decided.

Represented parties

Shealy conflicts with Tate Group and Fontainebleau on a party's own AI prep.

Expert prompts

CLF v. Shell ordered an expert's AI prompts produced; objection pending.

Spoliation and statutes

Krafton's damages phase; Arizona's AI-privilege bill stalled in 2026.

Questions

The companion memo has full analysis, citations, and the checklist.

Kimball Parker

Law current through November 9, 2026 · Not advice on any specific matter