PROGRAM MATERIALS
Program #36174
June 24, 2026

The AI Trap: How Legal Tech Tools Can Blow Up Confidentiality and Privilege

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

THE AI TRAP

How Legal Tech Tools Can Blow Up Confidentiality and Privilege

Angeli Raven Fitch, Esq.
AI Legal Strategist, 415-666-6189

This Is NOT an Anti-AI Talk

AI tools are transforming legal practice — drafting, research, discovery, and more

Early adopters gain real competitive advantage in speed and efficiency

But invisible risks are buried in Terms of Service, data flows, and default settings

What Is the AI Trap?

1

Using an AI Tool = Disclosing to a Third Party

Every AI vendor is a third party under ethics rules. When client information enters that system, you may have just violated Rule 1.6 (Confidentiality) — without your client's knowledge or consent.

2

Privilege Can Be Waived Permanently

Attorney-client privilege is lost when protected communications are voluntarily disclosed to a third party. Feeding privileged strategy, memos, or legal advice into an AI tool may strip that protection — retroactively and irreversibly.

3

The Data Leaves Silently — and You Can't Get It Back

Prompts, uploads, and documents travel to vendor servers and subprocessors before any answer returns. Once it's there, it may be stored, used for training, or accessed by vendor staff. There is no undo.

Why This Matters Right Now

77%

of law firms now use or are piloting AI tools

43%

of attorneys use AI tools NOT vetted by their firm

10

ABA ethics opinions on AI issued since 2023

0

states with comprehensive AI-specific legal ethics rules (yet)

Objectives today

01 Identify confidentiality and privilege risks in AI-assisted legal work

02 Apply ABA Model Rules 1.1, 1.6, 1.4, 5.1, and 5.3 to AI tool use

03 Evaluate vendor data practices and terms of service for client risk

04 Design safe AI workflows, policies, and privilege-preservation protocols

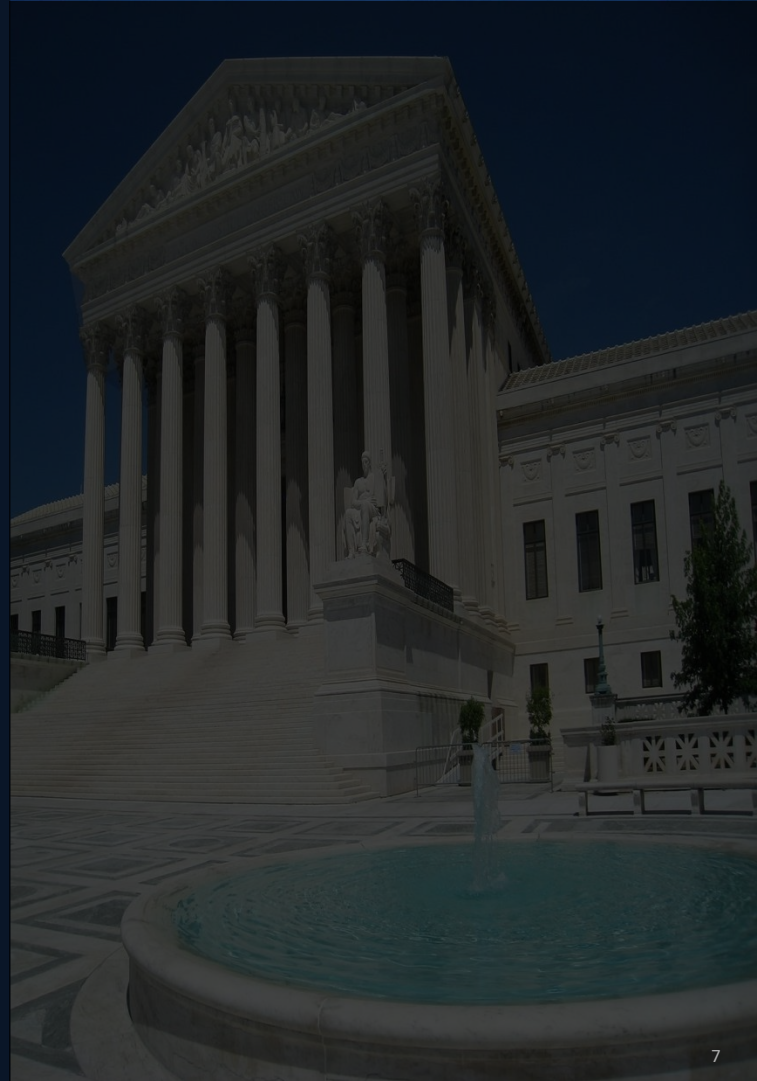
Today's Roadmap

PART 1	PART 2	PART 3	PART 4	PART 5
Where the Traps Are Hiding	Ethics, Confidentiality & Privilege	Follow the Data	Scenarios — Test Yourself	Build the Safeguards

PART 1

Where the Traps Are Hiding

Eight AI categories your clients are already using — and the risks inside each



The AI Tech Stack in Legal Practice

General AI Assistants	Legal Research AI	Contract Analysis
ChatGPT, Claude, Gemini	Westlaw AI, Lexis+ AI, Casetext	Kira, Luminance, ContractPodAi

Document Drafting	E-Discovery AI	Productivity Tools
Harvey, CoCounsel, Spellbook	Relativity, Everlaw, Disco	Microsoft 365 Copilot, Google Workspace AI

TRAP 1

General AI Assistants: The Invisible Disclosure

What attorneys actually do:

Type client names, facts, and strategy into ChatGPT or Claude to draft briefs, letters, and memos

Upload confidential contracts or pleadings for summarization or analysis

Use browser-based tools without reviewing default data retention settings

Why it is a trap:

OpenAI, Google, and others may use inputs to train future models — absent specific enterprise settings

Data may be stored on vendor servers in jurisdictions with different privacy laws

No attorney-client privilege attaches to communications with a third-party AI vendor

TRAP 2

Legal Research AI: Hallucinations and Attribution

- AI legal research tools cite cases that do not exist — attorneys have been sanctioned for filing them
- Even accurate citations can misstate holdings, ignore negative treatment, or omit critical qualifications
- Westlaw AI and Lexis AI market as 'hallucination-resistant' — but no system is hallucination-free
- Rule 3.3 (Candor to Tribunal) requires verification — reliance on AI output without checking is not enough
- Matter-level data shared with legal research platforms may be retained per vendor's terms

TRAP 3

Contract AI: Confidential Data in the Training Loop

Contract AI tools (Kira, Luminance, ContractPodAi) ingest full contract text to identify clauses

Some platforms use uploaded contracts to refine and train their models — check data processing addendums

Client contracts often contain trade secrets, pricing, and strategic terms — all potentially exposed

Many tools use subprocessors (cloud vendors, annotation services) with their own data rights

Due diligence requires reading the DPA (Data Processing Agreement), not just the ToS

TRAP 4

Document Drafting AI: The Ghost in the Brief

Harvey, CoCounsel, Spellbook and Claude for Legal integrate directly into Word and email — low friction means low caution

Drafts generated from confidential facts are transmitted to vendor servers with each query

Output quality varies — AI drafts may omit elements, misstate law, or use incorrect jurisdiction defaults

Supervision failures: attorney who merely reviews and files AI output without verification may violate Rule 1.1

Question: Who owns the AI-generated work product? Check your contracts carefully.

Traps 5 & 6: E-Discovery AI and Productivity Suites

E-Discovery AI (Relativity, Everlaw):

- Processes entire document sets — privileged docs may be exposed if logging is on
- AI-assisted privilege review can miss documents without human confirmation
- Predictive coding requires validation — inadvertent production waives privilege
- Vendor access to data for "support" purposes is a hidden risk

Productivity AI (M365 Copilot, Google AI):

- Already embedded in tools attorneys use daily — opt-in by IT, not the attorney
- Copilot indexes email, documents, Teams chats — all potentially processed by Microsoft
- Google Workspace AI similar: drafts, summaries, search all touch third-party servers
- Enterprise agreements may limit training use — but require affirmative enrollment

Traps 7 & 8: Communication AI and Client-Facing Chatbots

Communication AI (Otter.ai, Fireflies):

- Records and transcribes attorney-client meetings — third party now has the transcript
- Transcription stored on vendor servers, potentially indefinitely
- Meeting participants may not know they are being recorded — consent issues
- Transcript data used to improve vendor AI in some configurations

Client-Facing AI Chatbots:

- Intake chatbots gather legal facts before the attorney-client relationship is formed
- Data may flow to chatbot vendor, CRM, and lead management tools
- Unauthorized practice of law risk if chatbot provides substantive legal guidance
- Prospective client disclosures may be insufficient under Rule 1.18

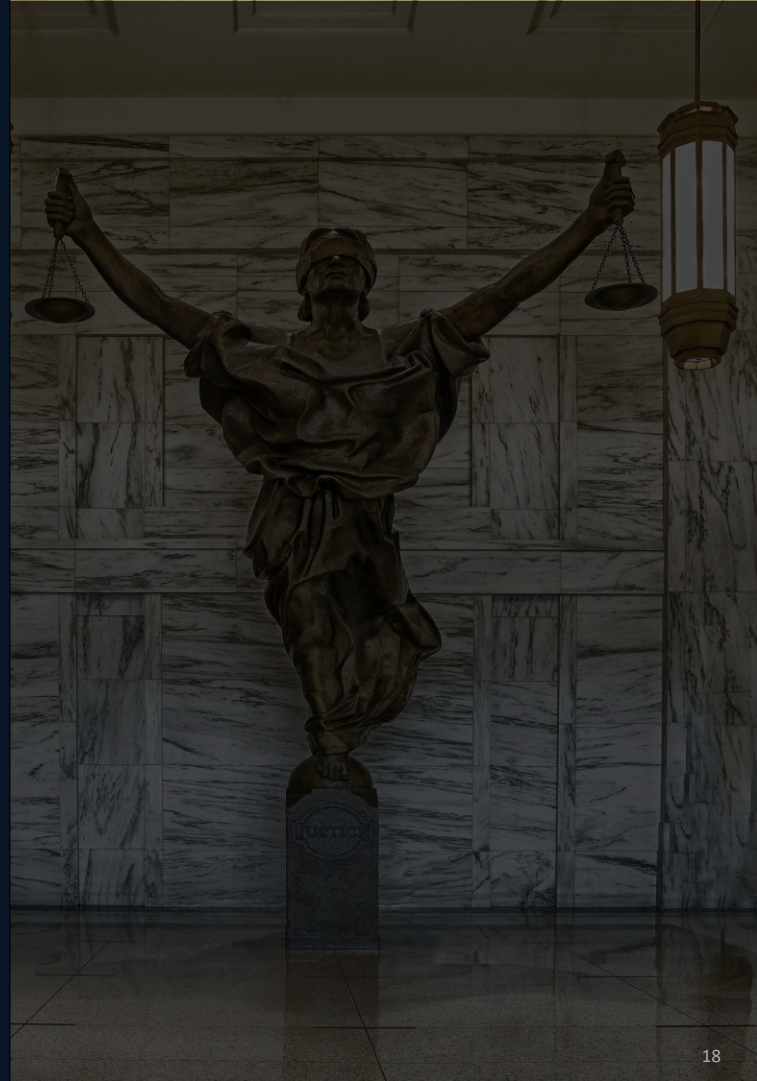
The AI Trap Taxonomy: Know What You Are Dealing With

Data Sharing	Client info sent to vendor servers	Rule 1.6
Training Use	Inputs used to improve AI models	Rule 1.6
Hallucination	False citations filed without verification	Rule 1.1, 3.3
Supervision Gap	AI output not reviewed before use	Rule 5.1, 5.3
Privilege Waiver	Disclosure to AI vendor = third party disclosure	Rule 1.6
Consent Failure	Client not informed of AI tool use	Rule 1.4

PART 2

Ethics, Confidentiality & Privilege

The rules, the opinions, and the duties that apply when AI meets client data



ABA Formal Opinion 512 (2024): The Foundation

Attorneys may use generative AI tools, but must take steps to ensure confidentiality of client information and apply appropriate supervision — the same as with any non-attorney assistant.

Competence (Rule 1.1): Understand the benefits AND risks of AI tools before using them

Confidentiality (Rule 1.6): Do not disclose client information without informed consent — AI vendors are third parties

Communication (Rule 1.4): Inform clients of material facts, including how their data is processed

Supervision (Rules 5.1/5.3): Partners and supervisors must oversee AI use by associates and staff

Fees (Rule 1.5): AI-assisted work product raises questions about billing — do not charge for time AI eliminated

Rule 1.1: Competence — Know the Tool You Use

Understand	How the tool processes and stores data
Evaluate	Whether the tool is appropriate for the matter type and sensitivity level
Verify	AI-generated output — citations, facts, legal conclusions — before filing or advising
Update	Your knowledge as AI tools and ethics guidance evolve (Comment 8: duty to keep current)

Rule 1.6: Confidentiality — The Core Prohibition

> *"A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized, or an exception applies."*

"Relating to representation" is BROAD — includes facts learned from the client, strategy, communications, and documents

Entering client data into an AI tool IS a disclosure to a third party unless you have a proper confidentiality agreement

Rule 1.6(c): Attorneys must make reasonable efforts to prevent unauthorized disclosure — which requires knowing where data goes

Implied authorization to share exists only for personnel necessary to provide services — AI vendors are not automatically included

Client consent: must be informed, which means explaining what the tool does and how data is handled

As a baseline, all lawyers should read and understand the Terms of Use, privacy policy, and related contractual terms and policies of any GAI tool they use….

— ABA Formal Opinion 512 (2024)

Rule 1.4: Communication — Do You Have to Tell Your Client?

Rule 1.4(b): Explain matters to the extent reasonably necessary to permit the client to make informed decisions

If AI use is material to representation — and it often is — clients should be informed

Increasingly, clients ASK: "Are you using AI on my matter?" — you need a clear answer and policy

Fee implications: if AI dramatically reduced hours, is the billable rate appropriate? Transparency required

Best practice: Include AI use disclosure in your engagement letter — what tools, how data is handled, client consent

Some jurisdictions (CA, FL) are moving toward requiring AI disclosure — get ahead of it now

Rules 5.1 & 5.3: Supervising AI Like You Supervise People

Rule 5.1 (Supervising Lawyers):

- Partners must ensure firm-wide measures to prevent AI-related ethics violations
- Cannot delegate responsibility for AI outputs — "the AI did it" is not a defense
- Must have policies: which tools are approved, what review is required, how data is handled
- Responsible for associate AI errors if no supervisory policies in place

Rule 5.3 (Supervising Non-Lawyers):

- AI tools are treated like non-lawyer assistants — must be supervised
- Staff using AI tools without attorney review creates ethics exposure for the supervising attorney
- Paralegal using ChatGPT for research? You are responsible for what gets filed
- Written policies and training are your best protection against supervision claims

Managerial lawyers must establish clear policies regarding the law firm's permissible use of GAI (generative AI).....

ABA Formal Opinion 512 (2024)

Rule 1.5: AI and Attorney Fees — The Billing Question

AI tools can reduce time dramatically — what does that mean for hourly billing?

Rule 1.5: Fees must be reasonable — billing for time an AI eliminated raises ethical questions

ABA has signaled: cannot charge full research rate for task AI completed in seconds

Options: (1) Pass savings to client; (2) Value billing; (3) Flat-fee arrangements for AI-assisted work

Cannot charge separately for AI tool costs AND bill full time — double recovery concerns

Transparency is the safest path: explain AI use and its effect on time in your bills

Confidentiality vs. Privilege: Critical Distinction

ETHICAL DUTY (Rule 1.6)

- Governs ALL client information
- Ethical rule — bar discipline
- Cannot be waived by attorney
- Does not require confidential communication
- Broader in scope

ATTORNEY-CLIENT PRIVILEGE

- Protects legal advice communications
- Evidentiary rule — court protection
- Can be waived by disclosure to 3rd party
- Requires confidential A-C relationship
- Narrower — but more powerful

Privilege Waiver: How AI Creates the Risk

Privilege is waived when confidential attorney-client communications are voluntarily disclosed to a third party without a compelling reason.

AI vendor = third party: uploading privileged communications to an AI tool may constitute voluntary disclosure

FRE 502 provides some protection from inadvertent waiver — but requires prompt remedial action

No court has definitively ruled on AI-assisted waiver — you do not want to be the test case

Cloud storage alone does not waive privilege — but sharing with a service provider that retains and uses data is different

Enterprise/BAA agreements may help — but only if you actually have one and it covers the specific use

Adversaries will seek AI interaction logs in discovery — treat them as potentially discoverable from day one

The Adversary's Lens: What Opposing Counsel Is Looking For

Discovery requests increasingly include: "All AI tools used in this matter and all data submitted to them"

Prompt logs, uploaded documents, and AI output may all be discoverable if not privileged

If you used AI to draft strategy memos, those inputs could be sought in discovery

Metadata in AI-assisted documents may reveal that AI was used and when

Sanctions risk: If AI-generated content was filed without verification and is inaccurate, sanctions are possible

Malpractice exposure: Clients harmed by AI errors (e.g., missed deadlines, wrong law applied) may have claims

Insurance: Does your malpractice policy cover AI-related errors? Check now, not after a claim.

State Bar Action: The Landscape Is Moving Fast

ABA Formal Op. 512 (2024): Foundational guidance on AI and confidentiality

California: State Bar issued practical guidance in 2023; rules revision underway 2026

Florida: Bar association issued AI ethics guidance; formal rules in progress

New York: NYSBA AI Task Force issued comprehensive report with recommendations

Texas: Task force studying AI ethics requirements for state bar members

Multiple states: Considering mandatory AI disclosure in court filings (following federal court orders)

Bottom line: Check your jurisdiction NOW — guidance is being issued faster than most attorneys track

Part 2 Summary: Your Ethics Checklist

1.1	Understand how each AI tool handles data before using it
1.6	Do not enter confidential client info without a proper DPA or enterprise agreement
1.4	Disclose AI use to clients in your engagement letter
1.5	Adjust fees fairly when AI eliminated significant time
5.1/5.3	Implement written AI policies; supervise all use by staff and associates
Privilege	Treat AI interaction logs as potentially discoverable from day one

PART 3

Follow the Data

Understanding where client information actually goes — and what you can do about it

Where Does Client Data Actually Go?

Prompts	Text you type is logged and may be retained for abuse monitoring, quality, or training
Uploads	Documents you attach are processed by the model and stored (duration varies by plan)
API Logs	Enterprise APIs may log requests; your IT team may not have disabled this
Integrations	Plugins, connectors, and third-party apps that access the AI all receive some data

The Six Data Flows You Must Understand

1. PROMPT DATA: Text input — may be retained for model improvement unless enterprise opt-out is active
2. UPLOADED DOCUMENTS: Files submitted for analysis — processed and stored on vendor infrastructure
3. CONVERSATION LOGS: Entire session history — may be reviewed by vendor for safety or quality
4. TRAINING DATA: Some vendors use inputs to fine-tune models — check ToS for current policy
5. INTEGRATION DATA: Third-party plugins and connectors receive portions of data with each query
6. SUBPROCESSOR DATA: Vendors use cloud infrastructure (AWS, Azure, GCP) and annotation services — each is a separate data handler

Reading Terms of Service: What to Look For

Training Opt-Out	Are inputs used to train models? Is opt-out available and is it the DEFAULT?
Data Retention	How long is data kept? Is there an enterprise setting to shorten or eliminate retention?
Subprocessors	Who else receives data? Is there a current subprocessor list? Can you object to changes?
Security Controls	What encryption, access controls, and certifications apply (SOC 2, ISO 27001, HIPAA)?
DPA / BAA	Is there a Data Processing Agreement available? Does it cover confidential legal data?
Jurisdiction	Where is data stored and processed? What law governs? Are there cross-border transfers?

The Privacy Policy Is Not the Same as the ToS

Privacy Policy governs personal data of end users — not necessarily CLIENT data entered by attorneys

Terms of Service governs what you can do with the product and how YOUR data (as the customer) is handled

Data Processing Agreement (DPA): The key document for attorney-client data protection — and most attorneys never ask for it

BAA (Business Associate Agreement): HIPAA requires certain entities to have one when protected health information (PHI) is shared with a third party. (Law firms often become business associates when representing hospitals, health plans, providers or other HIPAA-covered entities.

Important: Free and consumer tiers typically have MUCH weaker protections than enterprise/API tiers

Action: If a vendor will not provide a DPA for legal matters, treat that as a red flag — or use a different tool

Evaluating Vendor Security: What to Request

SOC 2 Type II Report: Proves security controls actually work (not just designed) — request annually

ISO 27001 Certification: International standard for information security management systems

Penetration Testing: Ask if vendor conducts regular pen tests and if you can see summaries

Encryption at Rest and in Transit: Both are required — confirm which encryption standards are used

Access Controls: Who at the vendor can access your data? For what purposes? With what logging?

Incident Response: How are breaches handled? What notification timelines apply? Do state breach laws apply to client data held by vendors?

Vendor Risk Tiers: A Framework for Your Firm

TIER 1 APPROVED	Enterprise agreement, DPA executed, training opt-out confirmed, SOC 2 reviewed, matter-level use approved
TIER 2 CONDITIONAL	Some protections in place; approved for non-confidential or anonymized use only; case-by-case review required
TIER 3 PROHIBITED	Consumer tools, no DPA, training opt-out not available, or insufficient security documentation

How Major Platforms Handle Attorney Data

Platform	Training Opt-Out	DPA Available	Default Retention
ChatGPT (Consumer)	Manual only	No	30 days + models
ChatGPT Enterprise	Yes (default)	Yes	Not used for training
Claude.ai Pro	Yes (default)	Yes (API)	Varies by plan
Copilot (M365 E3+)	Yes via admin	MSFT DPA	Per M365 policy
Westlaw AI	Yes	Thomson Reuters DPA	Contractual
Harvey (Law Firms)	Yes	Yes	Firm-controlled

Data as of June 2026. Verify current settings before use.

Subprocessors: The Hidden Data Chain

Every major AI vendor uses subprocessors — cloud providers, annotation services, safety reviewers

OpenAI subprocessors include: Microsoft Azure, Stripe, Salesforce, Twilio, and others

Your DPA with the AI vendor does not automatically flow to their subprocessors

GDPR Article 28: subprocessors must meet same data protection requirements as main processor

Action: Request current subprocessor list before executing DPA; require notification of changes

Annotation and RLHF (Reinforcement Learning from Human Feedback): Human reviewers may read samples of conversations for training — are yours included?

Bottom line: When you enter data, you are trusting not just the vendor but their entire supply chain

Data Retention: What Stays, What Goes, and Who Decides

Consumer AI tools: may retain conversation data indefinitely by default

Enterprise tools: typically allow firm-controlled retention windows (30, 60, 90 days or none)

Model training data: once used for training, practically impossible to delete from the model itself

Deletion requests: most vendors honor deletion of stored logs — but cannot delete data baked into model weights

Your obligations: state bar records retention requirements may conflict with vendor deletion schedules

Client data at end of representation: ensure data held by AI vendors is addressed in your file closing protocol

Key question: Does your AI vendor have a documented data deletion process you can trigger?

“

You are not just responsible for what you do with client data. You are responsible for what your vendors do with it.

Rule 1.1 Competence, Rule 1.6 Confidentiality

Cross-Border Data Flows: International Considerations

Most AI vendors are US-based — but may process data in multiple jurisdictions (EU, Asia)

GDPR (EU): Strict rules on cross-border data transfers; Standard Contractual Clauses required

UK GDPR: Similar restrictions post-Brexit; separate adequacy decisions required

Data localization: Some jurisdictions require client data to stay in-country — check for your clients

Canadian PIPEDA / Quebec Law 25: Privacy requirements for Canadian client data

Practice point: If your client operates internationally, their data flowing through US AI tools may create violations abroad

PART 4

Scenarios: Test Yourself

Real-world situations — would you catch these issues in practice?

SCENARIO 1

The Research Memo

An associate at a 40-attorney firm uses ChatGPT (free tier, personal account) to draft a research memo on a pending merger involving a publicly traded client. She pastes in the client's name, the target company, and key deal terms to get the analysis started. She reviews the output and files the memo in the client matter. The partner is pleased with the turnaround time.

► **DISCUSSION: Has a Rule 1.6 violation occurred? What should the firm do now? What policies would have prevented this?**

SCENARIO 2

The Filed Brief

A solo practitioner uses an AI legal research tool to find supporting cases for a motion to dismiss. The tool returns five cases with proper citations. He pastes the citations directly into the brief and files it. The court clerk calls the next day — two of the five cases do not exist in Westlaw or Lexis.

► **DISCUSSION: What ethics rules apply? What are the attorney's obligations now? What is the potential exposure?**

SCENARIO 3

The Meeting Transcript

A transactional attorney uses Otter.ai to record and transcribe all client meetings for convenience. The engagement letter does not mention this. A client later learns his strategy discussion — including a sensitive business dispute he had not disclosed publicly — was transcribed and stored on Otter's servers.

► **DISCUSSION: Is there a Rule 1.6 issue? A Rule 1.4 issue?**

SCENARIO 4

The Contract Upload

A partner at a mid-size firm signs up for a contract AI tool for the firm without IT or ethics review. She uploads 200 client contracts for analysis. The tool's ToS states: "We may use anonymized contract data to improve our services." The vendor later publishes a blog post referencing deal structures that closely resemble her client's proprietary arrangements.

► **DISCUSSION: What violations may have occurred? Is "anonymized" enough protection?**

SCENARIO 5

The Privilege Log

During discovery, opposing counsel serves a request for all AI tools used in the matter and all prompts submitted to those tools. The firm used Copilot to assist drafting strategy emails and privilege log entries. The firm's IT logs show the prompts, which contained client strategy and facts about the litigation.

► **DISCUSSION: Are the prompts discoverable? Is privilege waived? What arguments do you have? What should you do right now?**

Scenario Debrief: Key Takeaways

1. Consumer-tier AI tools are almost never appropriate for confidential client matters
2. Every AI-generated citation must be independently verified before filing
3. Recording and transcription tools require client disclosure and consent
4. "Anonymization" by vendors is not a legal protection — it is a marketing term
5. AI interaction logs must be treated as potentially discoverable from day one

The best time to think about AI ethics is before you use the tool. The second best time is right now.

— AI Legal Strategist — CLE Program 2026

What These Scenarios Have in Common

In EVERY scenario, the violation could have been prevented by three things:

1. A firm-wide AI policy — with an approved tools list and prohibited uses
2. An attorney who understood the risk BEFORE using the tool
3. A client engagement letter that addressed AI use, consent, and data handling

None of these require technical expertise. They require intentionality.

The attorneys in these scenarios are not bad lawyers — they are uninformed ones.

After today, you have no excuse not to know.

PART 5

Build the Safeguards

Practical policies, protocols, and workflows to protect your clients — and your practice

The Safe AI Workflow: Five Gates

GATE 1	GATE 2	GATE 3	GATE 4	GATE 5
Vet the Tool	**Classify the Data**	**Check Settings**	**Verify Output**	**Document Use**
Is it on the firm approved list? If not, stop here.	Is the information confidential, privileged, or PII? If yes, only Tier 1 tools.	Is training opt-out active? Is the enterprise account in use — not personal?	Human review of every AI-generated work product before use. No exceptions.	Log that AI was used, which tool, and the verification step taken.

Matter-Level AI Rules: Tailoring Use to Each Client

Not all matters carry the same risk — your AI policy should reflect this

Highly sensitive matters (M&A, litigation, IP, criminal): Written approval required

Standard matters (drafting, research): All tools require human supervision

Public-domain or non-confidential work: Broader tool access may be appropriate

Engagement letter: Include AI consent provision that explains tool categories, data handling, and right to opt out

Matter opening checklist: Add AI classification step — what tier is appropriate for this client and matter type?

Client-specific restrictions: Some clients (government, regulated industries) will prohibit AI use — capture and enforce these

Staff Training: What Everyone Needs to Know

ALL STAFF

- Approved tools list and where to find it
- Never use personal AI accounts for firm work
- Report suspected AI-related incidents immediately

ATTORNEYS

- Ethics obligations under Rules 1.1, 1.6, 1.4, 5.1
- How to verify AI-generated citations and content
- Privilege implications of AI use in litigation

ADMINS & IT

- How to configure enterprise AI settings (opt-outs, retention)
- Incident response protocol for AI data breaches
- Vendor review and DPA execution process

The Human Review Requirement: Non-Negotiable

AI output is a DRAFT, not a work product — it requires attorney review before any use

Review checklist for legal research: (1) Verify citations exist; (2) Read the actual case; (3) Check negative treatment; (4) Confirm it applies to your jurisdiction

Review checklist for drafts: (1) Verify all factual statements; (2) Confirm law is current; (3) Check for internal consistency; (4) Apply professional judgment

Documentation: Note that AI was used and human review was completed — this protects you if challenged

Speed caution: If AI is saving time, do not fill that time by reducing review quality — use it to go deeper

Delegation: Associates may use AI but partners must review with the same rigor as any associate work product

Privilege Preservation in the AI Era

1. Use enterprise accounts — personal accounts do not have the contractual protections needed
2. Execute a DPA before using any AI tool for privileged matters — document it in the matter file
3. Label AI interaction logs as "Attorney Work Product" in your matter management system
4. Limit disclosure: only attorneys and supervised staff should see AI-generated strategy content
5. Confidentiality agreements: consider adding AI tool use to NDA and confidentiality agreement language with clients
6. Litigation hold: when litigation is anticipated, address AI interaction logs in your litigation hold notice
7. FRE 502(d) Orders: seek protective orders in litigation that explicitly address AI-assisted work product

AI Incident Response: When Something Goes Wrong

STOP	Cease use of the tool immediately; preserve logs and screenshots
ASSESS	Determine what data was exposed, to whom, for how long, and whether a DPA was in place
NOTIFY	Contact your ethics hotline or bar counsel; consult your malpractice carrier; assess client notification obligations
REMEDIATE	Request vendor data deletion; issue litigation hold if needed; evaluate FRE 502 implications
DOCUMENT	Record every step taken — demonstrates good faith and reasonable measures
REFORM	Update your AI policy, approved tools list, and training based on what you learned

Your 30/60/90 Day AI Ethics Action Plan

30 DAYS	• Audit: List every AI tool your firm uses (ask everyone) • Classify each tool by tier (approved/conditional/prohibited) • Identify any tools operating without a DPA — stop use or get agreement
60 DAYS	• Draft written AI use policy — approved list, prohibited uses, supervision requirements • Update engagement letter template — add AI consent and data handling disclosure • Conduct firm-wide training on this material (or adapt this CLE)
90 DAYS	• Review DPAs for all Tier 1 tools — execute or renegotiate • Add AI classification step to matter-opening checklist • Establish AI incident response protocol and designate responsible attorney

THE BOTTOM LINE

AI will not replace lawyers.
Lawyers who use AI responsibly will replace those who do not.

Angeli Raven Fitch, Esq.

Use AI | Vet AI | Supervise AI | Protect Clients

Sources & CLE Disclaimer

- ABA Formal Opinion 512 (2023) — Generative Artificial Intelligence Tools
- ABA Model Rules of Professional Conduct — Rules 1.1, 1.4, 1.5, 1.6, 3.3, 5.1, 5.3
- ABA TechReport 2023 — Legal Technology in Law Firms
- California State Bar — Practical Guidance for the Use of AI (2023)
- New York State Bar Association — AI Task Force Report (2024)
- Federal Rules of Evidence, Rule 502 — Attorney-Client Privilege and Work Product
- OpenAI, Anthropic, Microsoft, Thomson Reuters — Current Terms of Service and Privacy Policies
- GDPR Article 28 — Processor and Subprocessor Requirements

DISCLAIMER: This presentation is prepared for CLE educational purposes only and does not constitute legal advice. Attendees should independently verify all information and consult their own state bar ethics resources. AI tool terms and vendor practices change frequently — verify currency before reliance.