

Can Texas Lawyers Upload Client Files to ChatGPT?

Austin Bar Association | Stephen Walther



This session is for educational purposes only and does not constitute legal advice. I am not a lawyer. Consult a licensed attorney for guidance on specific legal matters. No guarantees are made regarding accuracy or outcomes.

Who I Am



MIT / Harvard

PhD Research on
Artificial Intelligence



Ex Microsoft

Led development of
Microsoft's web
developer platform



Book Author

Author of several best-
selling technology
books

Questions for You

Who has used AI for legal work?

- ChatGPT?
- Claude?
- Gemini?
- Harvey/Legora/CoCounsel?

**How many of you have entered
information about a client into an AI
system?**

Thesis

Question:

Can I safely use consumer ChatGPT?

Answer:

Not as part of a professional legal workflow.

AI in Legal Practice: Maturity Levels

Maturity
Level

LEVEL
1



Consumer AI

(ChatGPT, Claude, Gemini)

General-purpose tools for individual use.
Not designed for legal practice.

LEVEL
2



Enterprise AI

(ChatGPT Enterprise, Claude Enterprise)

Stronger security, privacy, and admin controls for the organization.

LEVEL
3



Legal AI Platforms

(Harvey, Legora, CoCounsel)

Purpose-built for legal work with domain expertise and workflow tools.



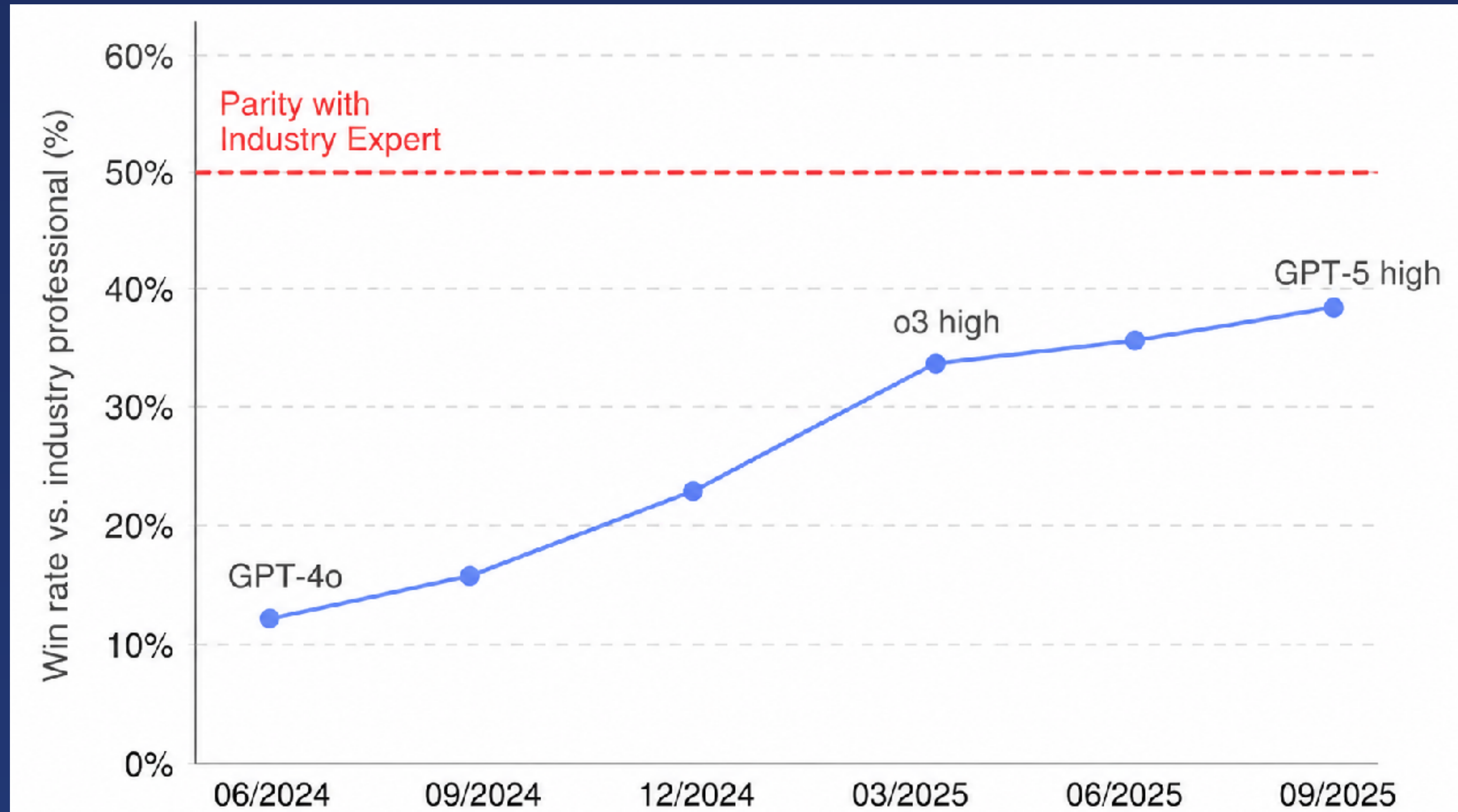
Firm-specific AI (Custom)

Built around your firm's unique workflows, knowledge, and practices.

Is the AI Hype Justified?

AI Is Transforming Every Knowledge Profession

Frontier AI models are rapidly approaching expert-level performance on real professional work.



Source: OpenAI GDPval (2025)

My experience with AI

I've spent over 30 years building software.

**The way I write software today is completely different
than it was two years ago.**

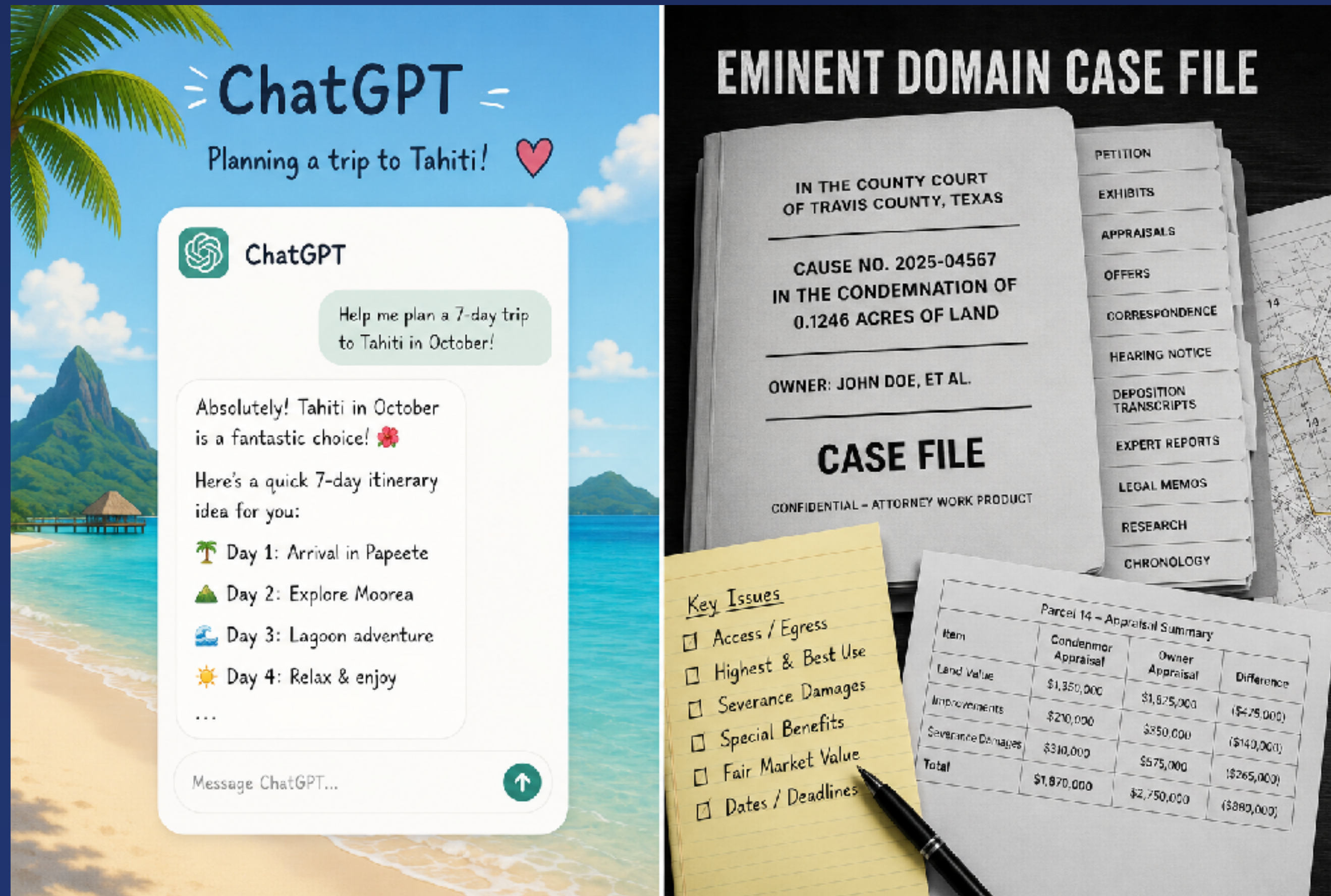
Generative AI Saves Time

Based on a survey of 2,800 legal professionals:

- 65% saved **1 to 5 hours** per week
- 12% saved **6 to 10 hours** per week
- 7% saved **11 or more hours** per week

But consumer AI is not recommended for
professional practice

The Wrong Way: ChatGPT



A tool designed to help plan a trip to Tahiti is not the right foundation for professional legal work.

**ChatGPT, Claude, Gemini = general
purpose, consumer tools**

(Nothing wrong with that, but you would not
give a brain surgeon a Swiss Army knife)

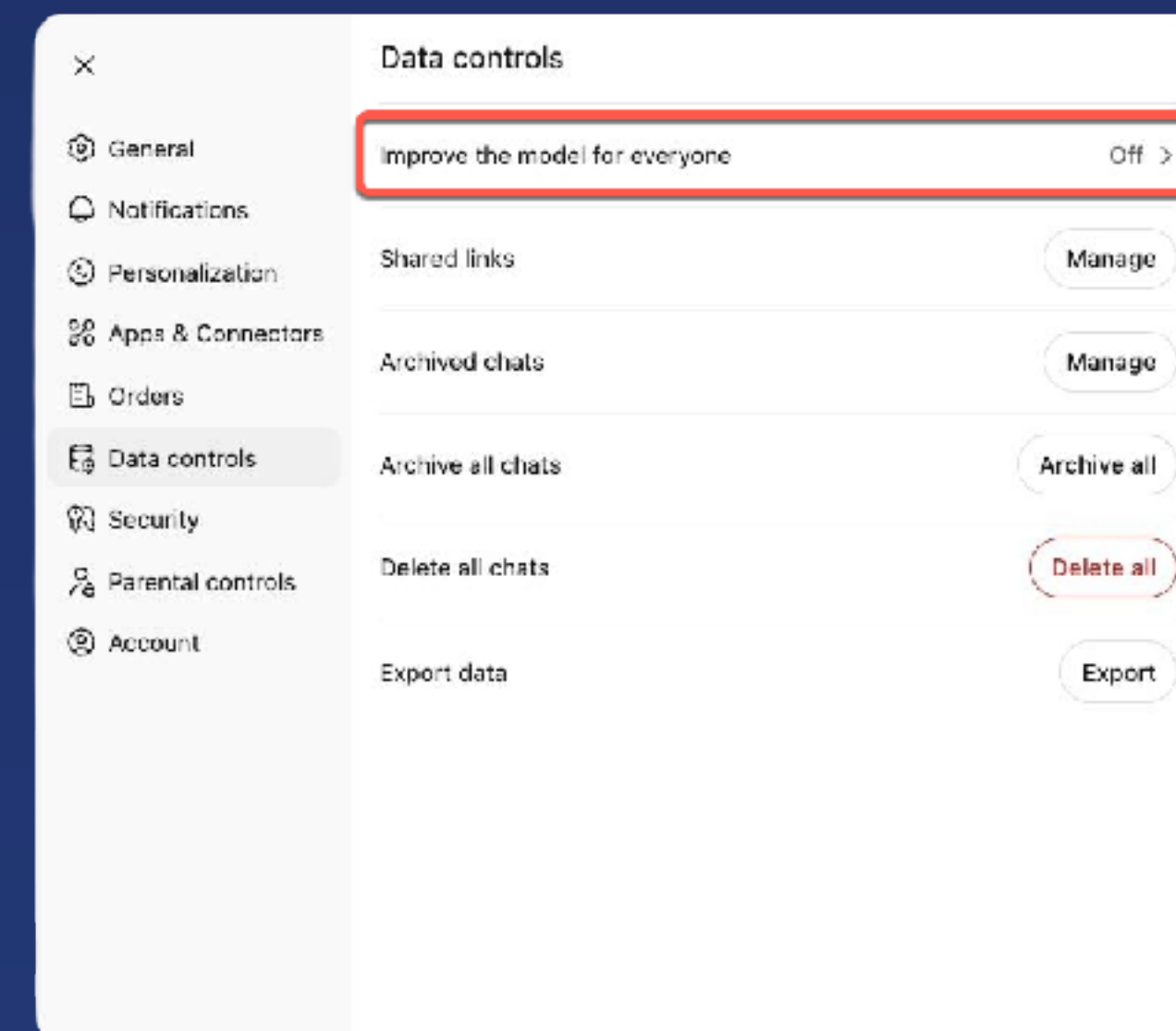
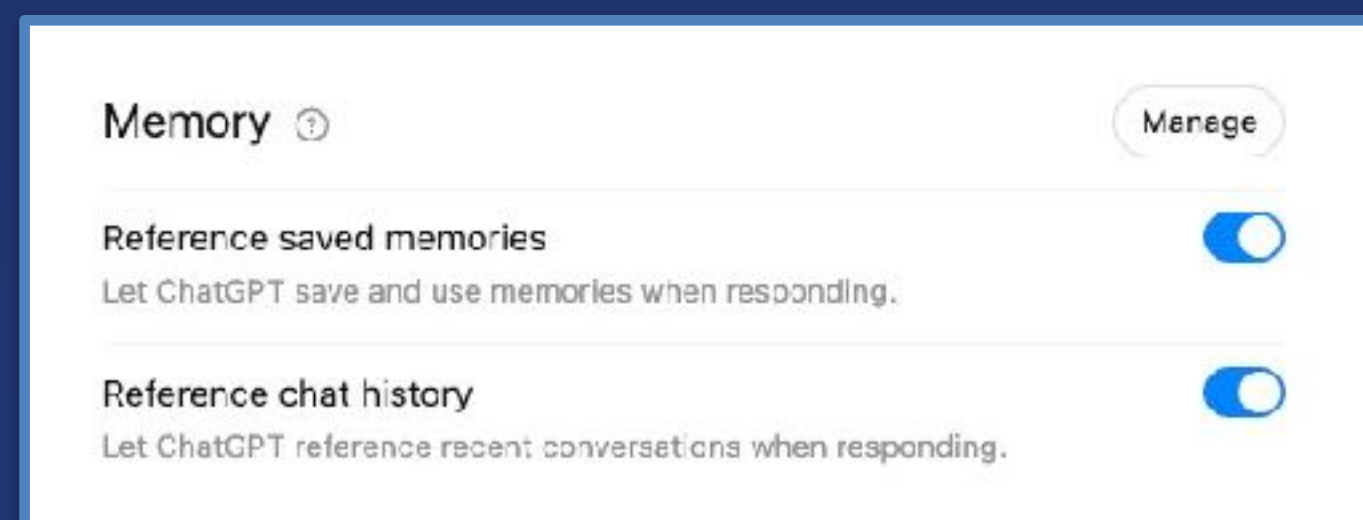
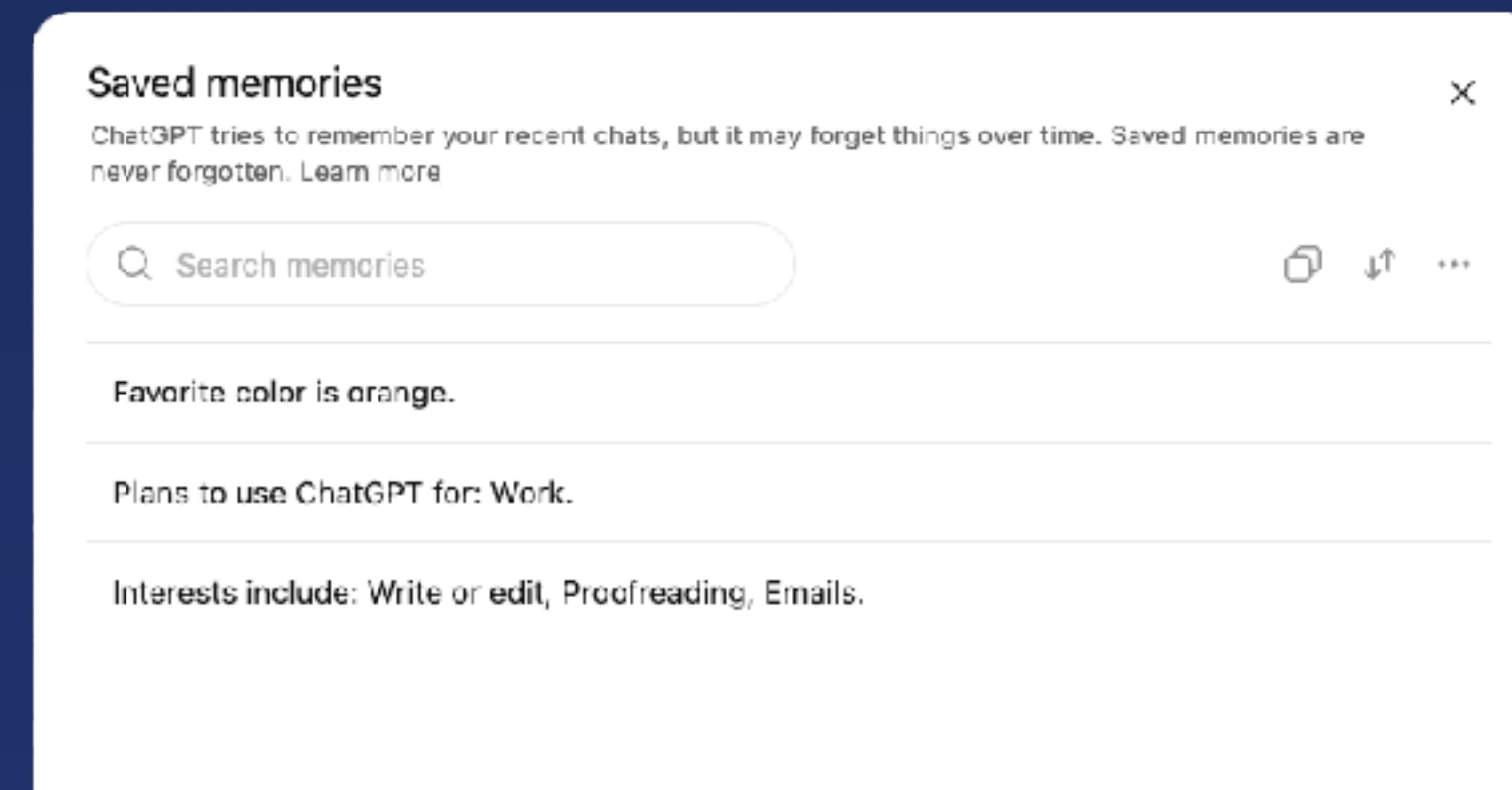
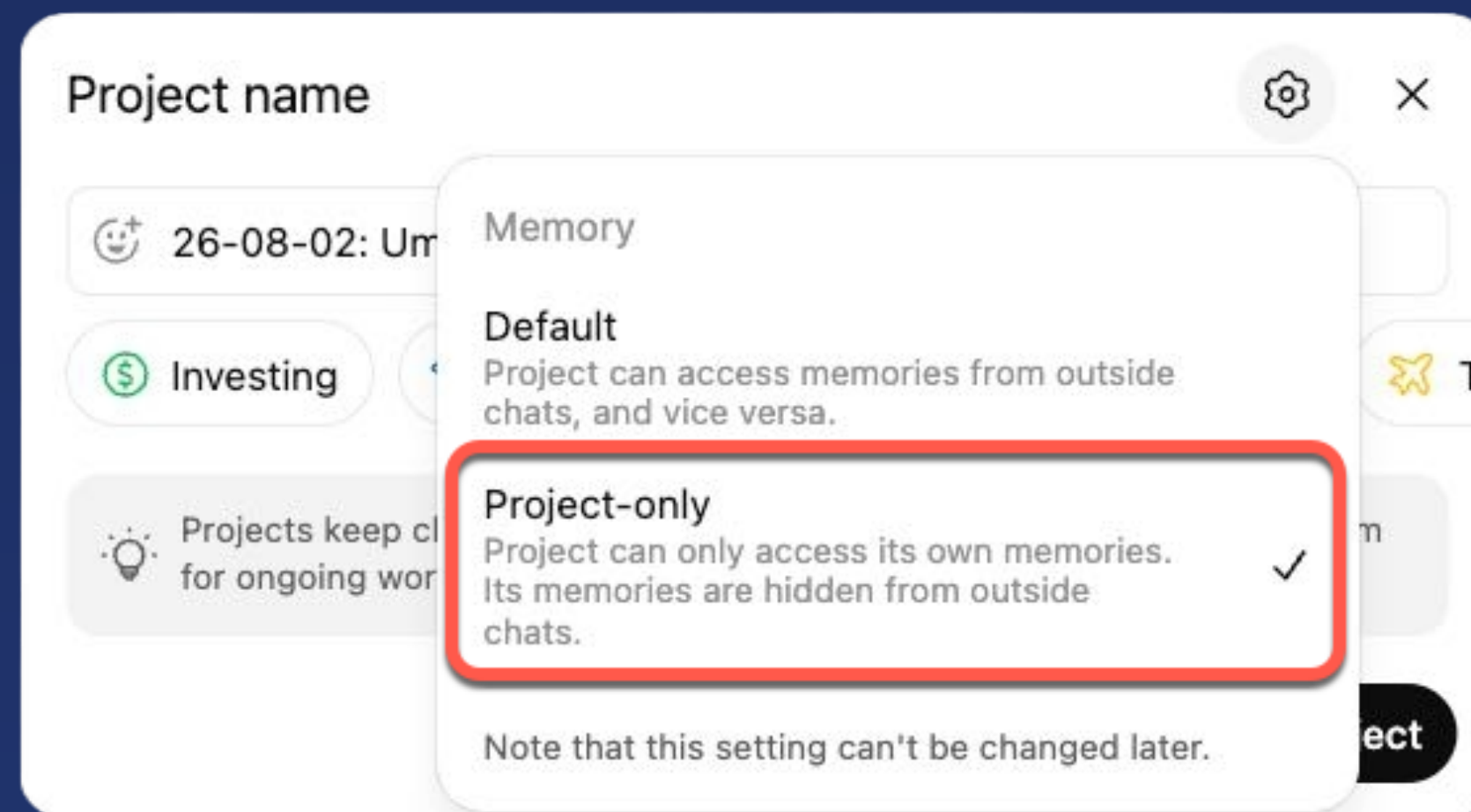
ChatGPT risks mixing matters



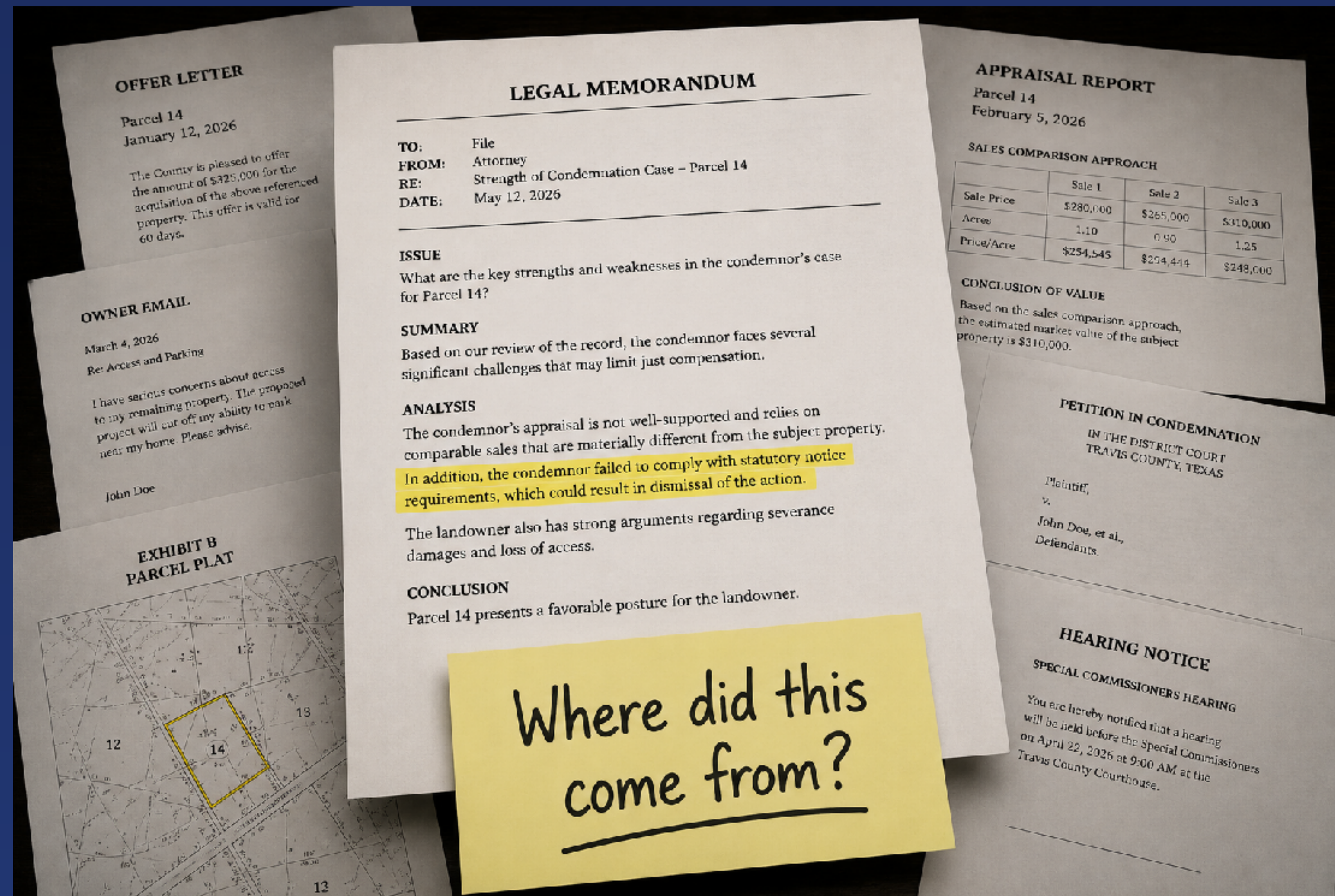
Legal work begins with matter isolation.

ChatGPT was not designed around legal matters.

Even Projects require the right configuration and careful use.



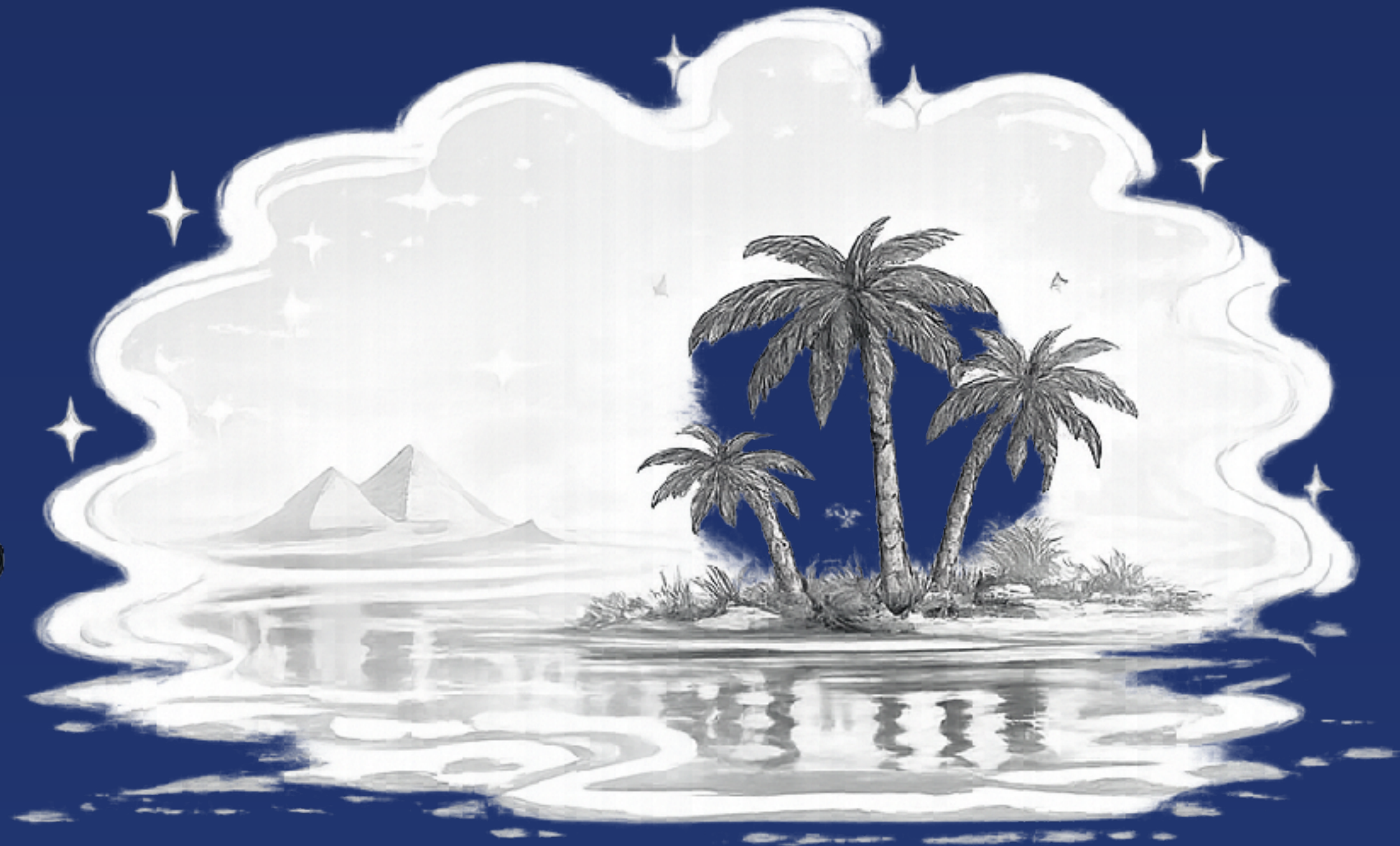
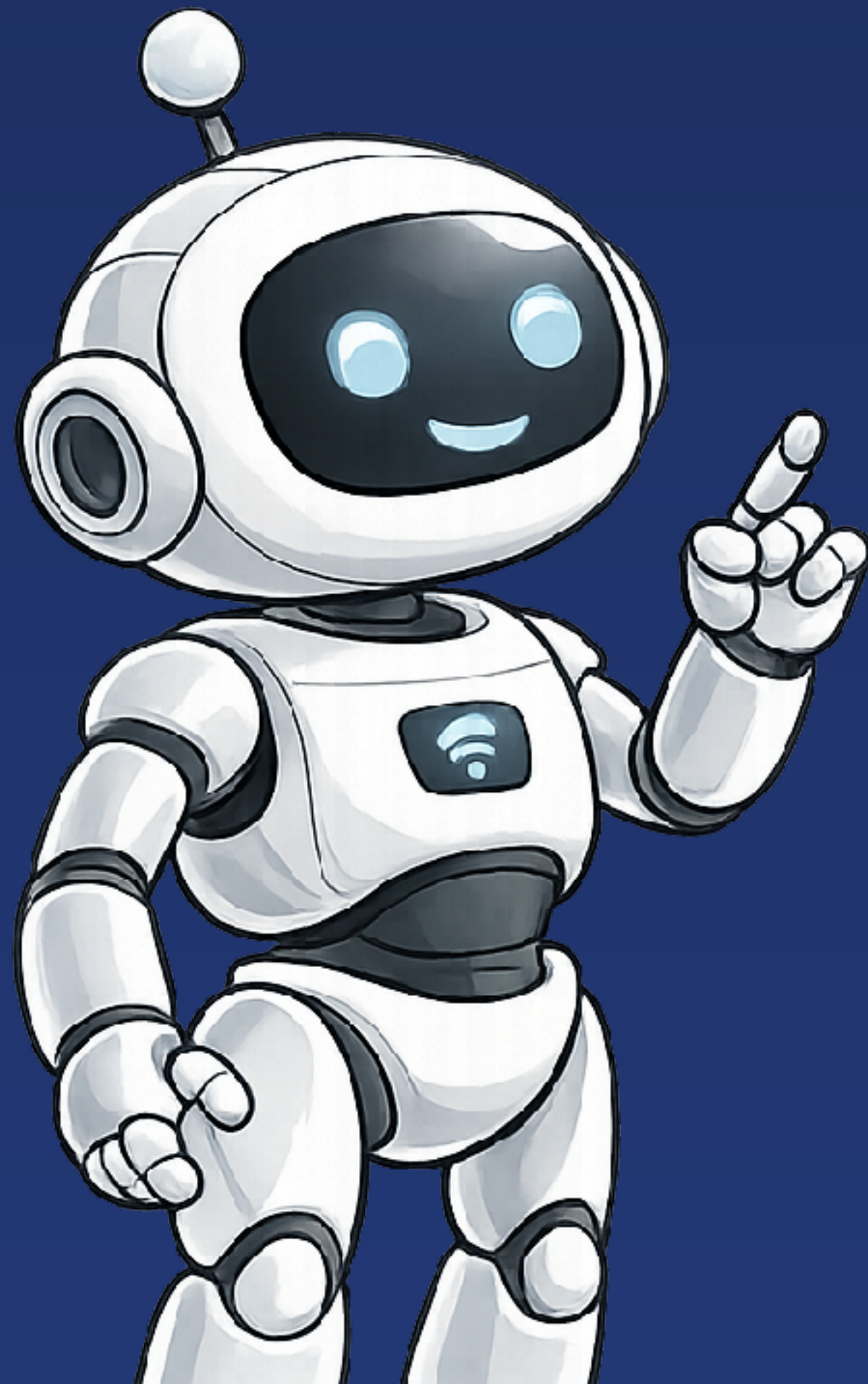
ChatGPT hallucinates



Every important claim should lead back to the record.

What Hallucinations Are (and Why They Happen)

A hallucination is a confident-sounding output that is not grounded in your sources



Real-World Consequences for Lawyers



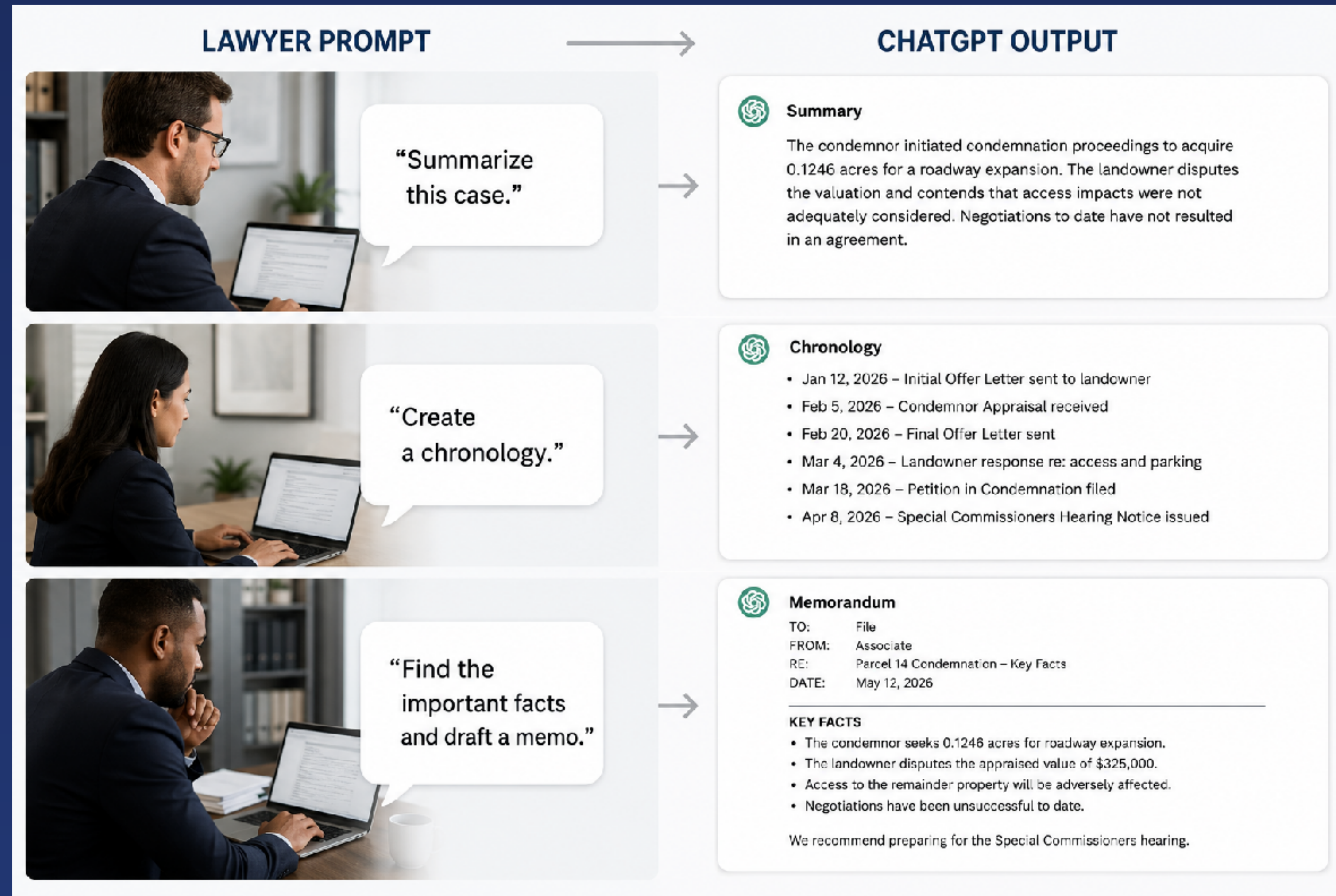
By Evan Gorelick

Nov. 7, 2025

Earlier this year, a lawyer filed a motion in a Texas bankruptcy court that cited a 1985 case called *Brasher v. Stewart*.

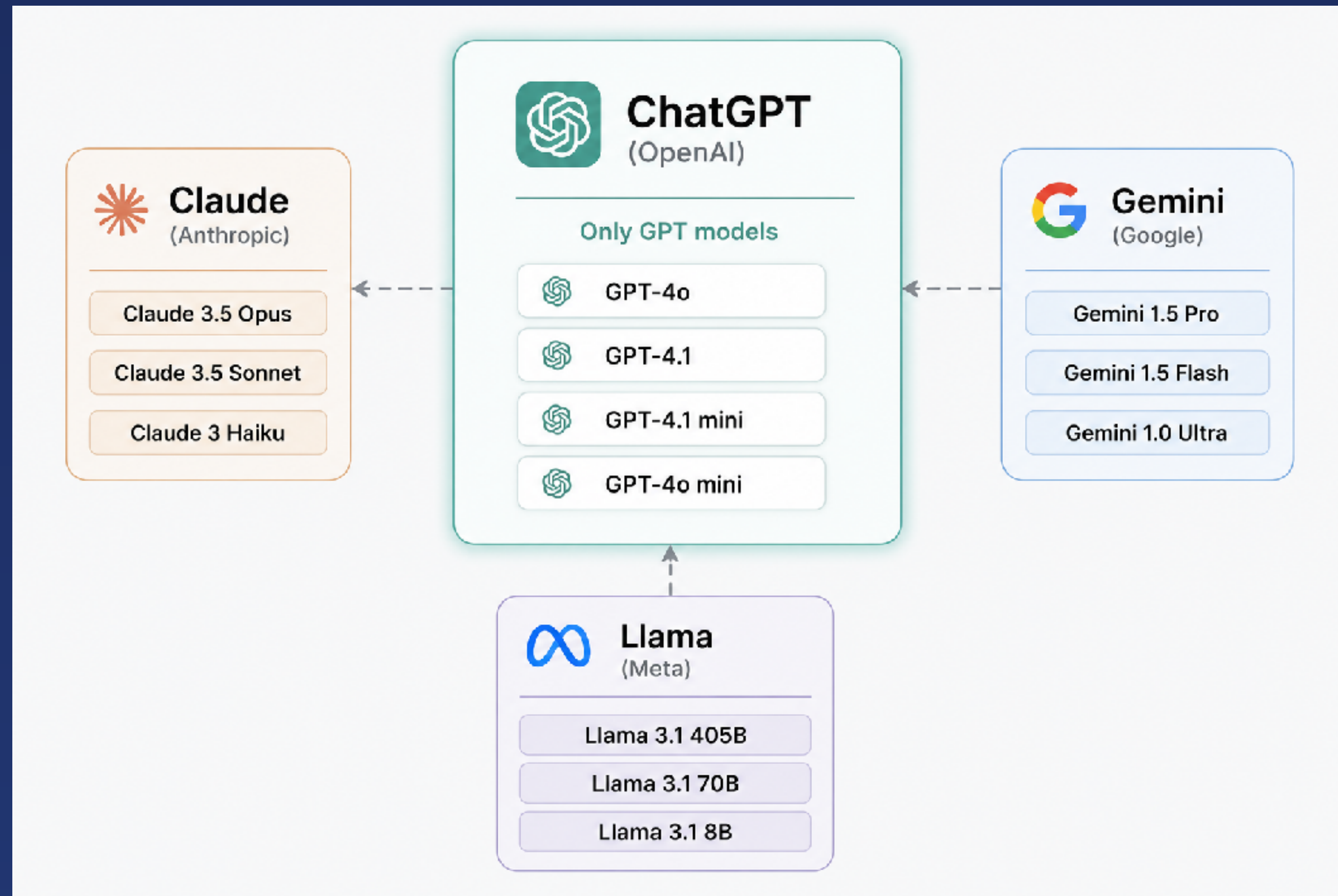
Only the case doesn't exist. Artificial intelligence had concocted that citation, along with 31 others. A judge blasted the lawyer in an opinion, referring him to the state bar's disciplinary committee and mandating six hours of A.I. training.

ChatGPT does not support Repeatable Workflows



A prompt is not a process.

ChatGPT limits you to OpenAI models



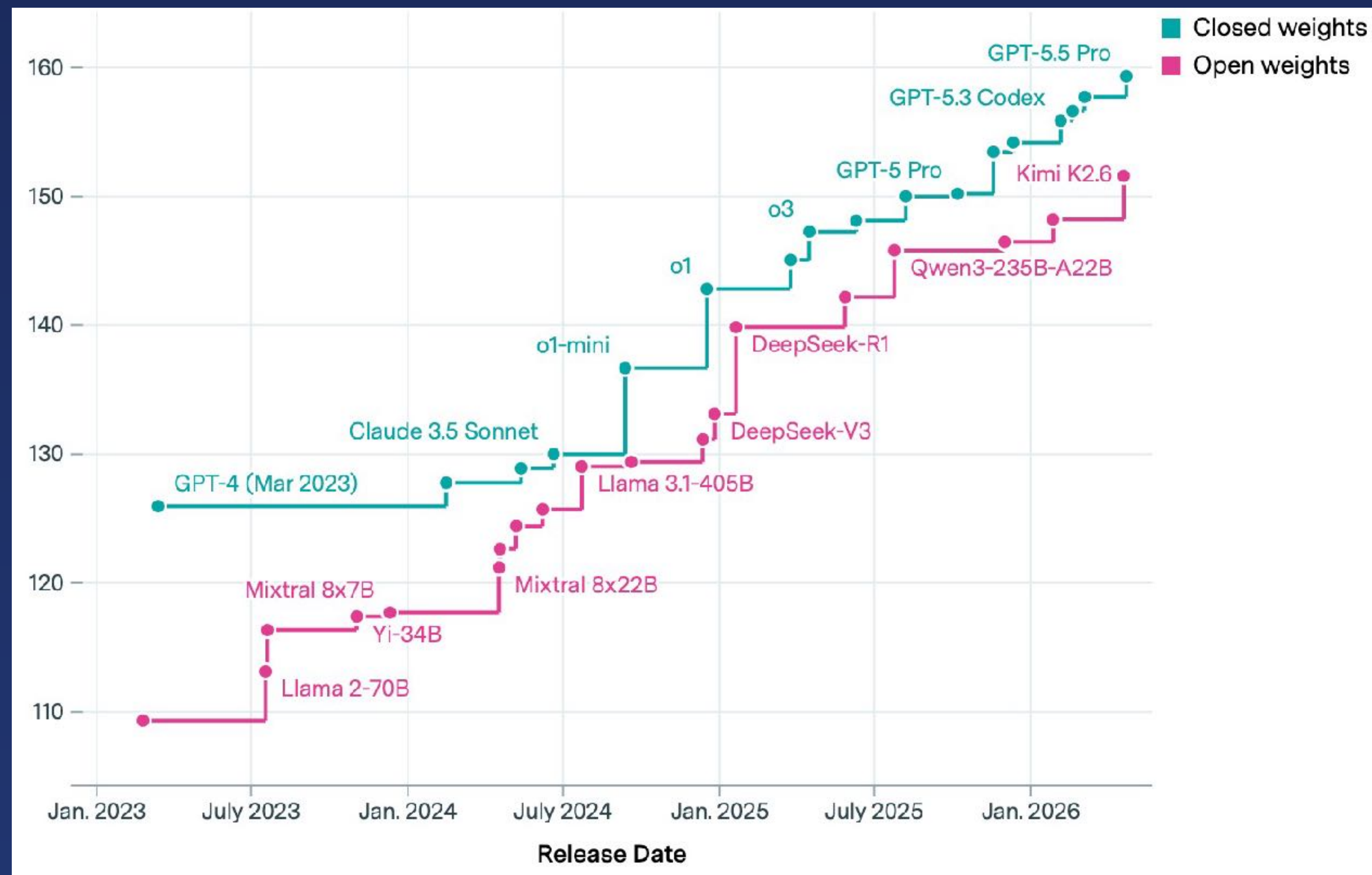
Different tasks need different models.

Models vary in reasoning ability, speed, context capacity, deployment options, and cost.

ChatGPT requires sending client data over the Internet



Local models can run inside the firm's own environment.



Local models lag state of the art models
by 4 months.

These Concerns are Reinforced
by Texas Opinion 705

What the Ethics Rules Emphasize

Texas Opinion 705

- Competence
- Confidentiality
- Supervision & Verification
- Court Rules
- Fees

Why Generative AI supports competence

- *Lawyers should not unnecessarily retreat from the use of new technology that may **save significant time and money for clients**.*

— Texas Opinion 705

- *It is conceivable that lawyers will eventually **have to use [GAI]** to competently complete certain tasks.*

— ABA Opinion 512

The ethics rules do not prohibit AI use; they constrain how it is used

Ethics Guidance Treats Confidentiality as the Primary Risk

“Some of the greatest risks posed by the unthinking use of generative AI relate to confidentiality of client information.”

— *Texas Ethics Opinion 705*

Risks include both:

- Exposing client information outside the firm
- Accidental co-mingling of information across client matters

It's surprisingly easy to reveal confidential client information

- “Rewrite this demand letter to sound more persuasive.”
- “Summarize this deposition transcript.”
- “Help me draft a motion based on these medical records.”

What about Work Product?

Are AI conversations, prompts, transcripts, logs, and outputs protected work product?

TRCP 192.5(a)(1) distinguishes:

- **Core Work Product** - An attorney's or their representative's mental impressions, opinions, conclusions, or legal theories. This is generally absolutely protected from discovery.
- **Other Work Product** - Factual materials prepared or mental impressions not involving core attorney thought processes. These are discoverable only if the opposing party shows a "substantial need" for the material and that they would face "undue hardship" to obtain it via other means.

Recent Cases

Stronger Protection

Tate Group (Texas)

AI prompts reflecting legal strategy protected as core work product.

Warner / Morgan

AI is a tool. Using AI alone does not waive work product.

Less Protection

Heppner

Public Claude use outside counsel direction. Privilege and work product rejected.

Conservation Law Foundation

Expert prompts ordered produced as part of expert methodology.

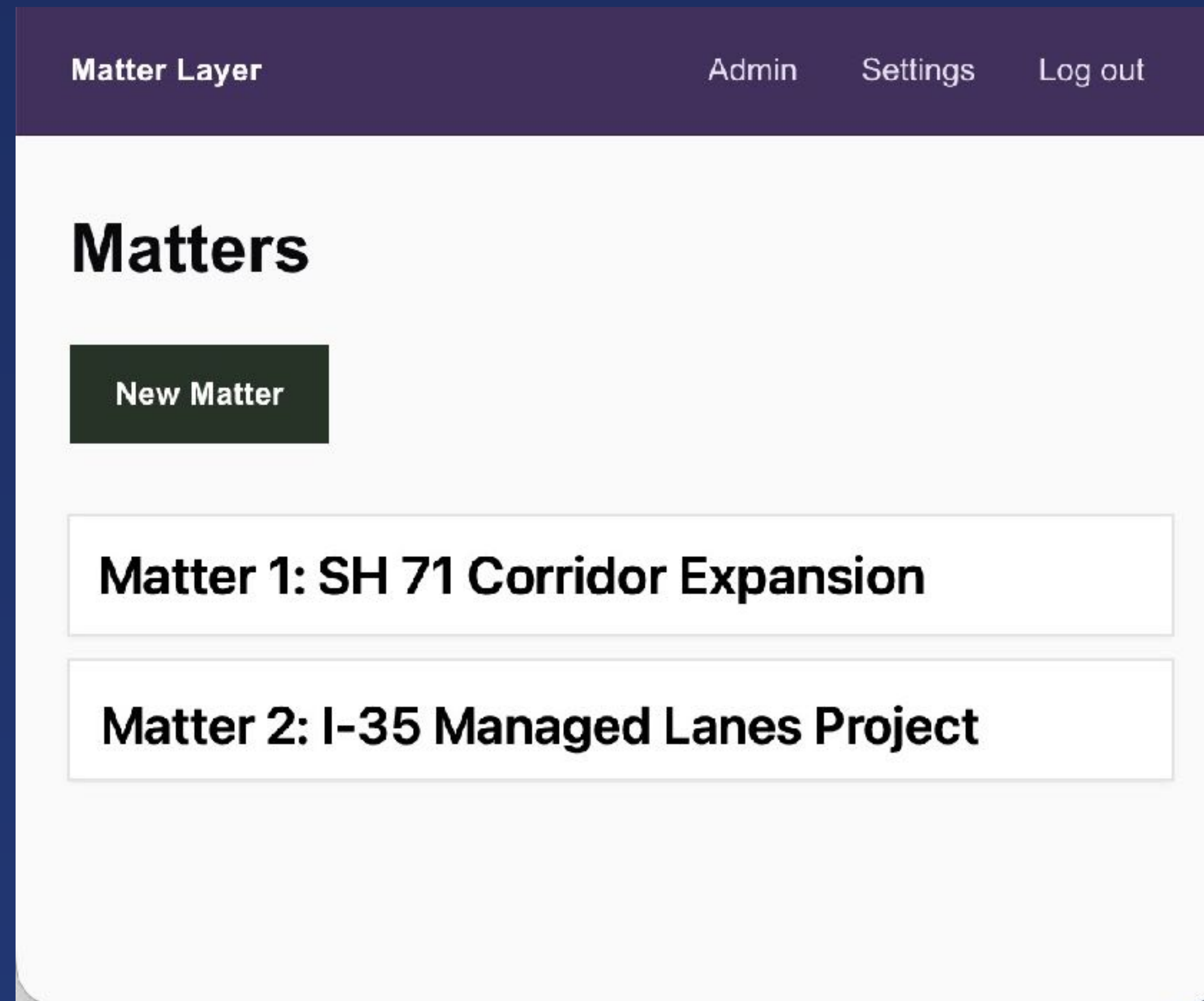
Practical Takeaways

- AI prompts revealing legal strategy receive the strongest work product protection.
- Consumer AI tools like ChatGPT and Claude present the greatest confidentiality and discovery risks.
- Choose the AI maturity level that matches the client's confidentiality requirements.
- The law surrounding AI and work product is still developing.

Four Requirements for Professional Legal AI

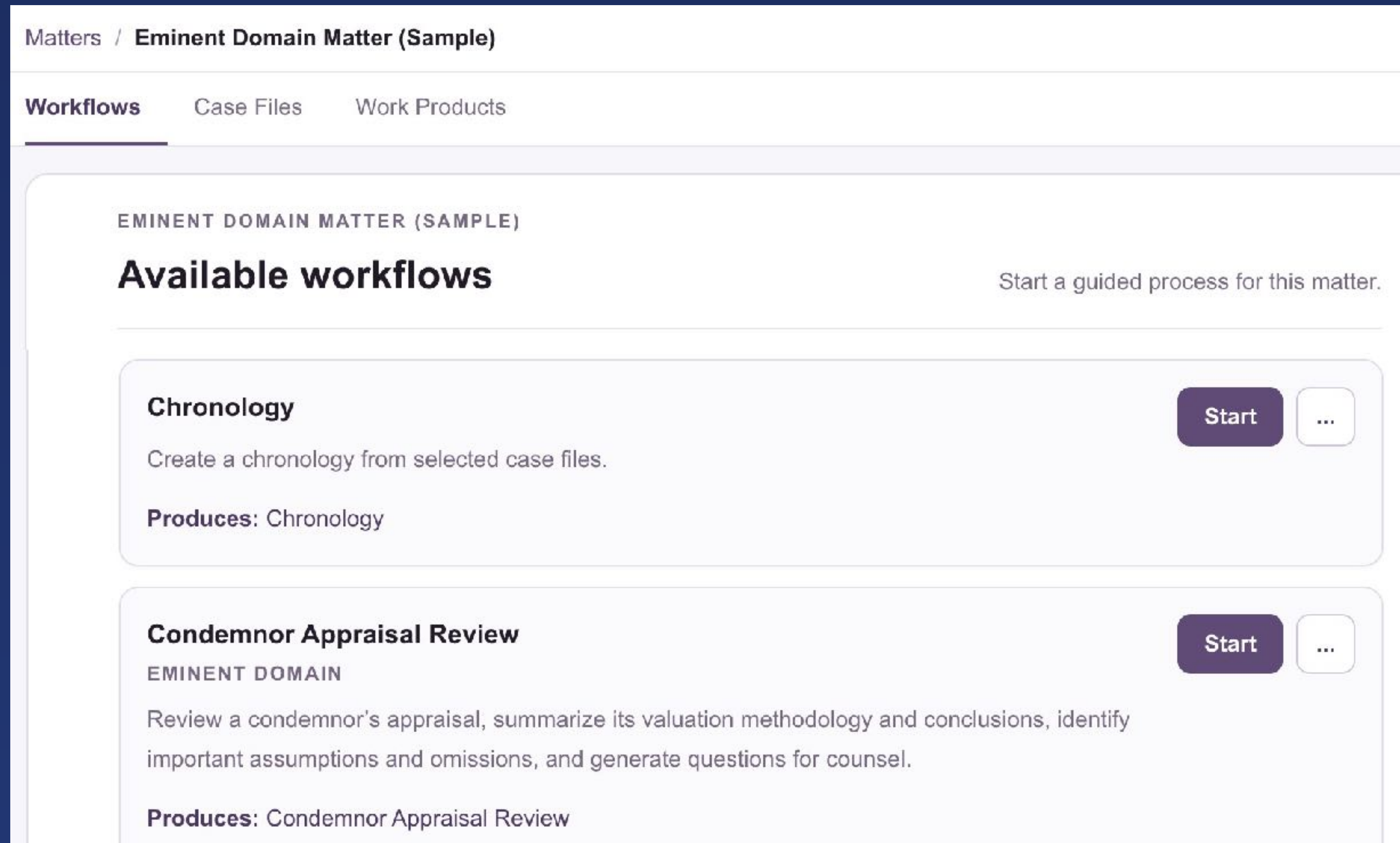
Requirement #1

Professional AI must isolate every matter.



Requirement #2

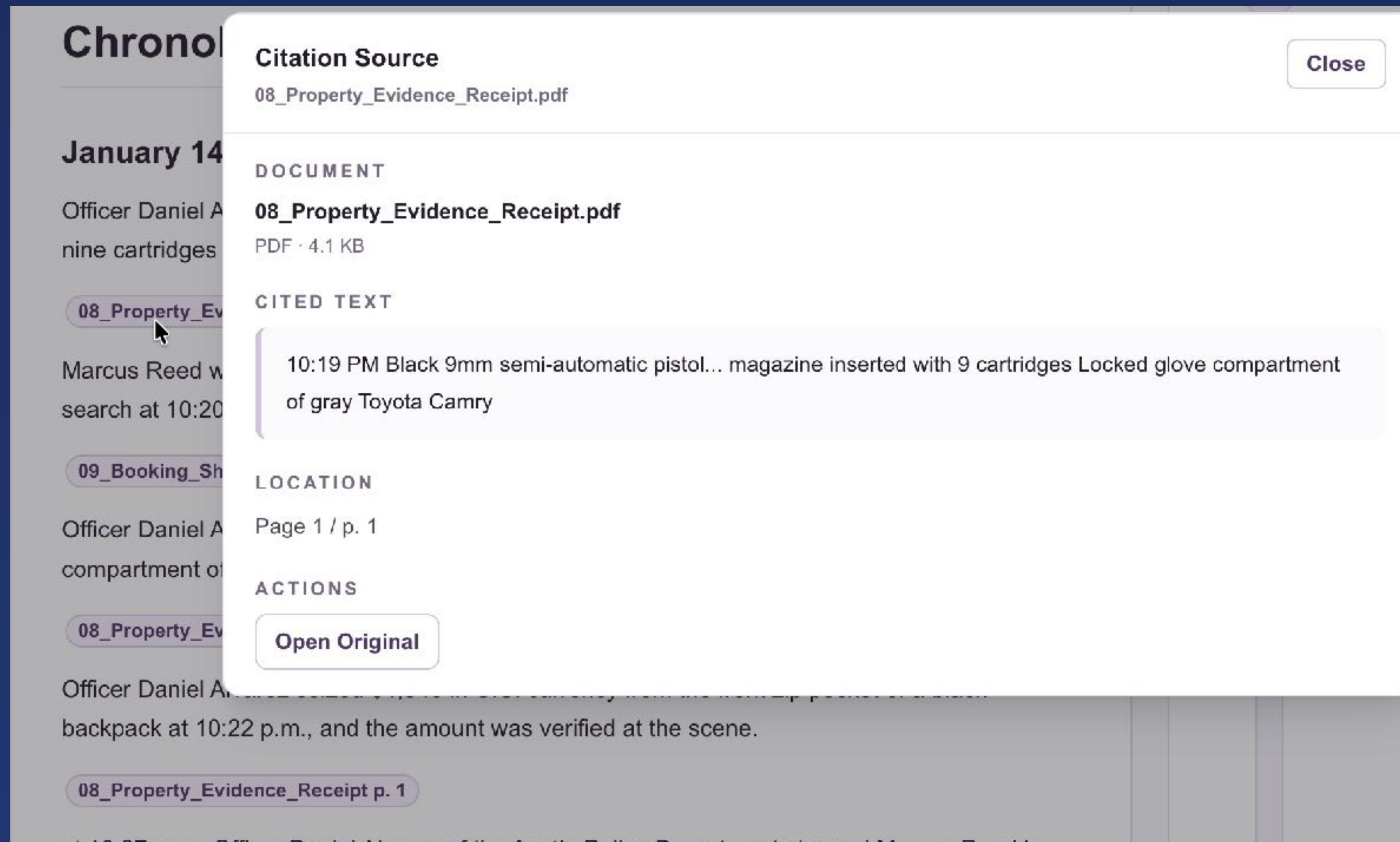
Professional AI should enforce repeatable workflows.



Workflows, not chat, should be the focus.

Requirement #3

Professional AI must ground every conclusion in evidence.



Professional AI should never ask you to trust it. It should show you the evidence.

Matters

New Matter

Eminent Domain Matter (Sample)
Criminal Matter (Sample)

Requirement #4

Professional AI should support different AI models for different tasks.

OpenAI Active

Model

GPT-5.6 Luna

API key

.....eI_ecA

Activate another provider before deleting this one.

Test

Delete

Ollama Local

Model

gemma3:4b

Server

http://localhost:11434

Test

Make active

Delete

Anthropic

Model

Claude Sonnet 4

API key

.....TbHQAA

Make active

Delete

Including local models when the security demands require it.

Consumer AI

Professional AI

Chat

Matter

Prompt

Workflow

Trust AI

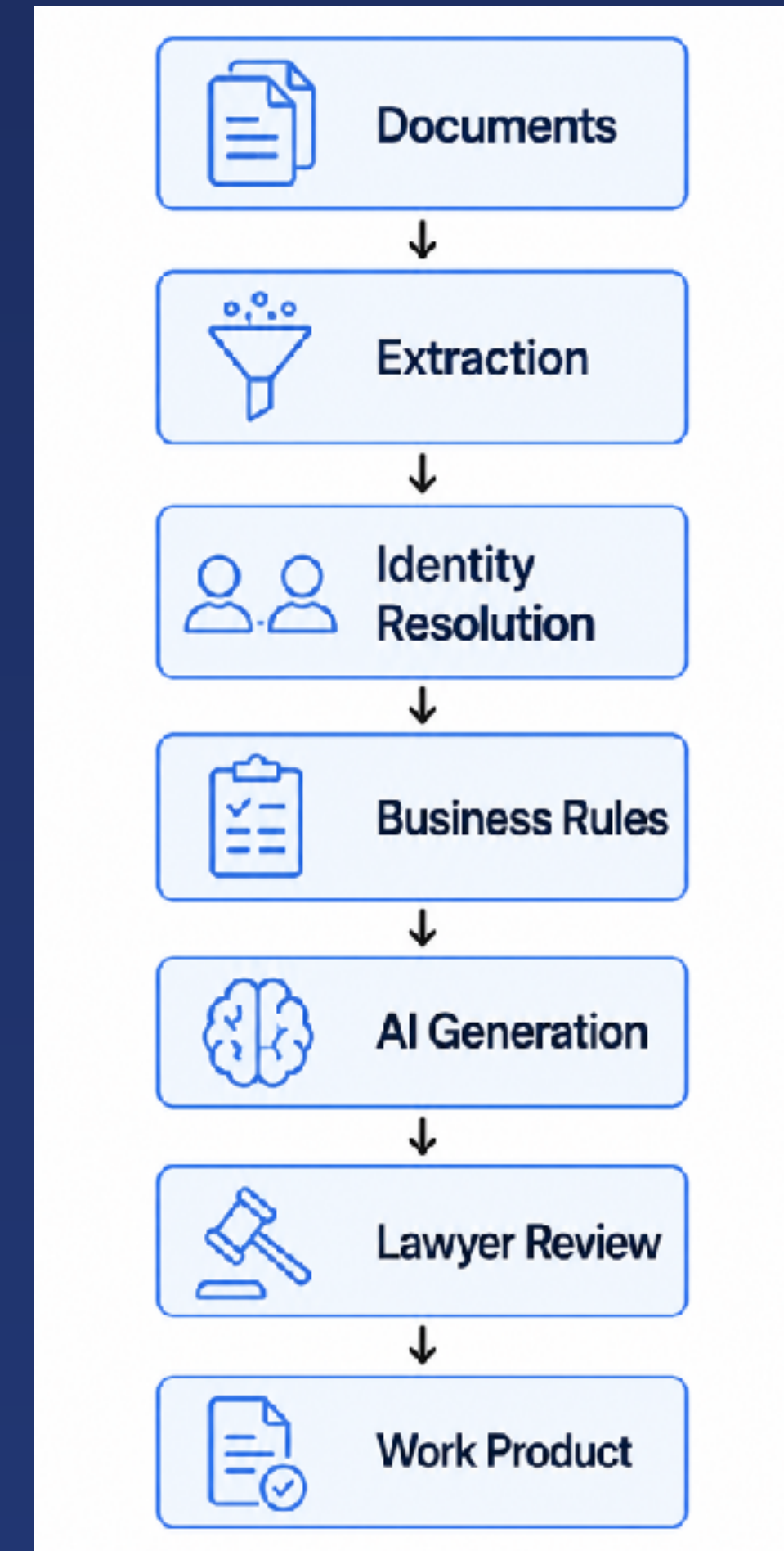
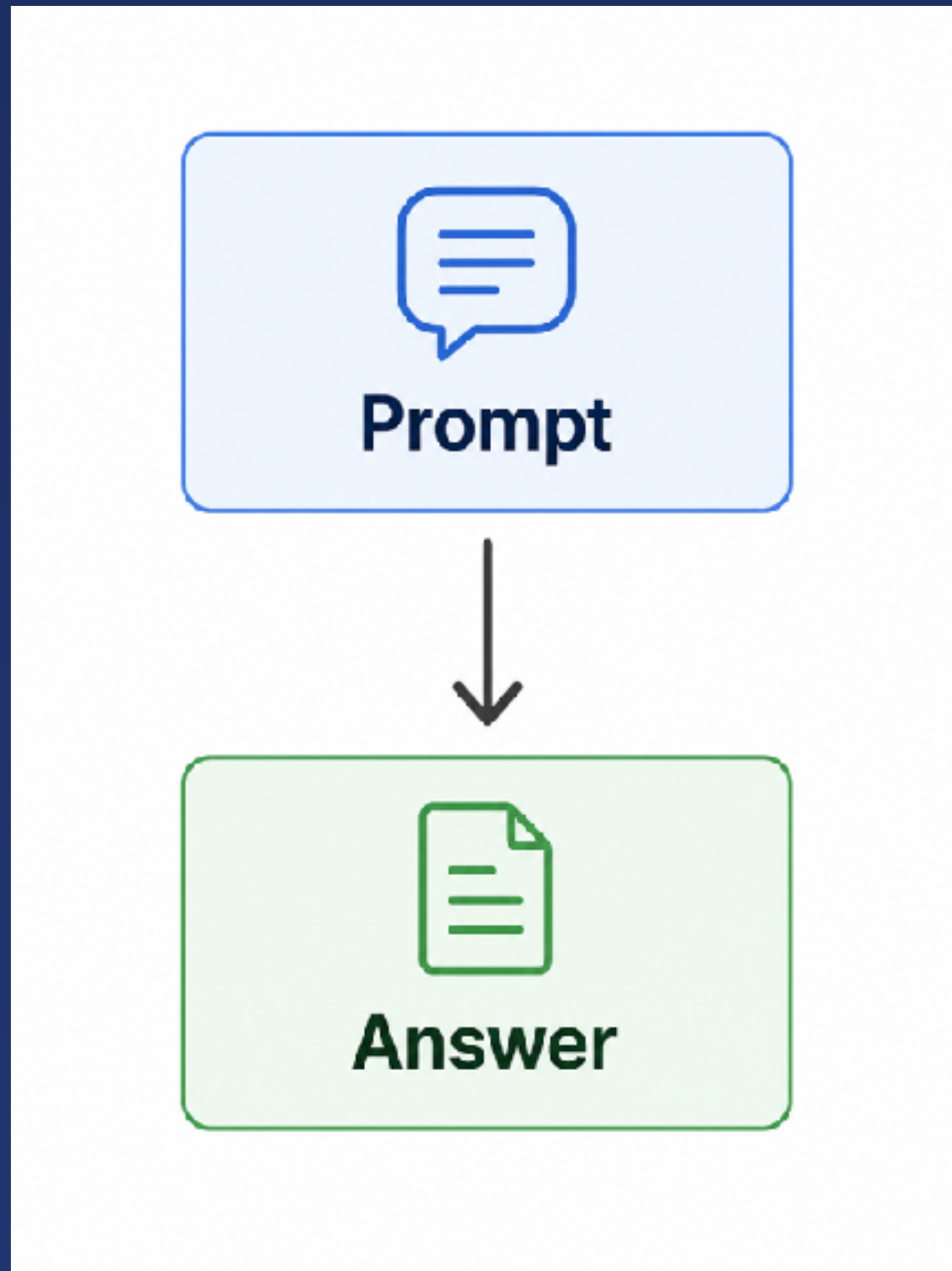
Verify the evidence

One vendor

Multiple models

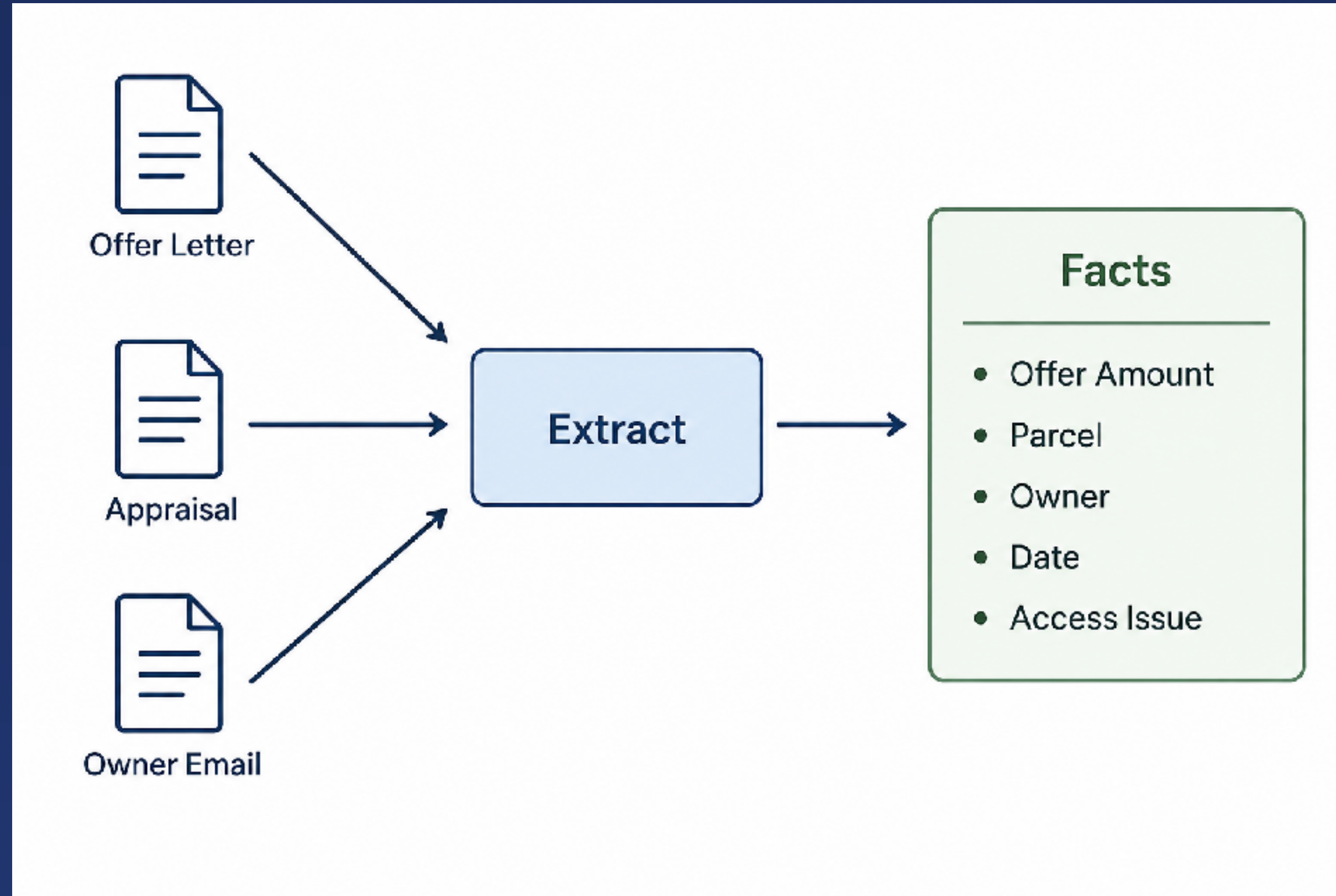
Why isn't a workflow just a
collection of prompts?

A prompt is not a workflow



This is why software engineering still matters.

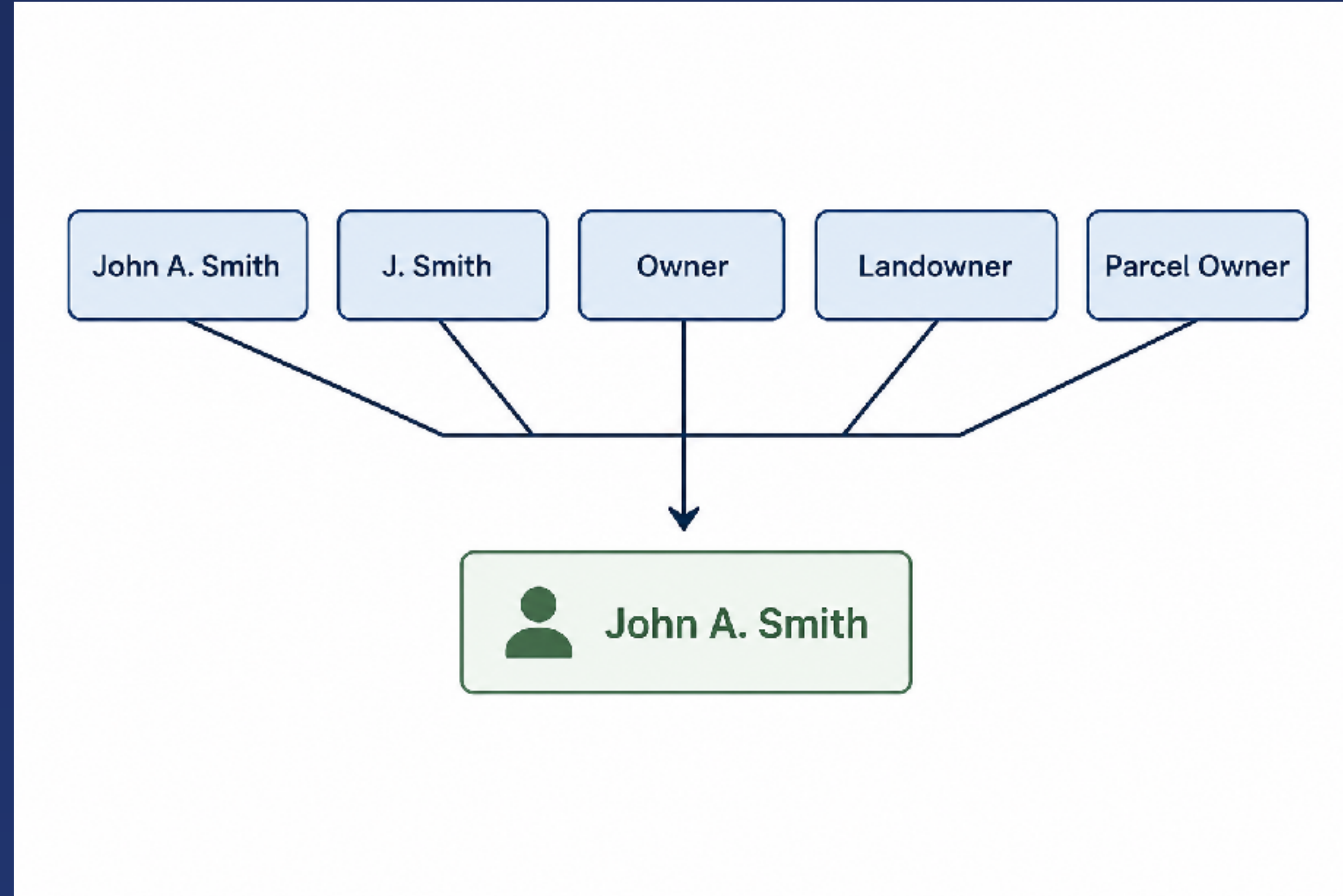
Step 1 - Structured Extraction



Why prompts aren't enough:

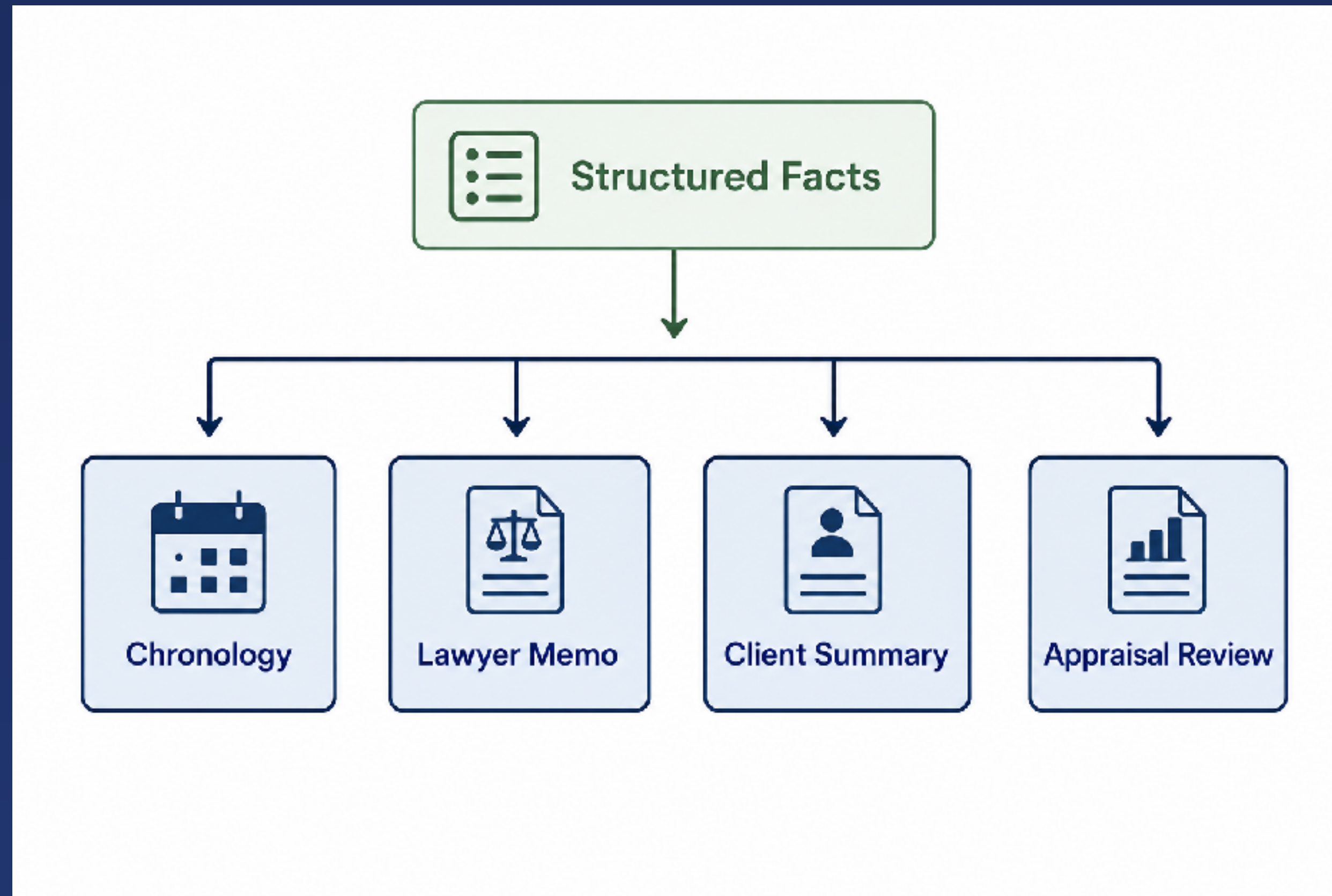
- AI cannot accurately reason over hundreds of pages directly.
- It first converts documents into structured facts.

Step 2 - Identity Resolution



AI doesn't automatically know that "John Smith," "Owner," and "Landowner" are the same person...that requires engineering.

Step 3 - Work Product Generation



Once information is structured, many different work products can be generated from the same facts.

Enterprise AI

AI in Legal Practice: Maturity Levels

Maturity
Level

LEVEL
1



Consumer AI

(ChatGPT, Claude, Gemini)

General-purpose tools for individual use.
Not designed for legal practice.

LEVEL
2



Enterprise AI

(ChatGPT Enterprise, Claude Enterprise)

Stronger security, privacy, and admin controls for the organization.

LEVEL
3



Legal AI Platforms

(Harvey, Legora, CoCounsel)

Purpose-built for legal work with domain expertise and workflow tools.



Firm-specific AI (Custom)

Built around your firm's unique workflows, knowledge, and practices.

Enterprise AI (ChatGPT/Claude Enterprise)

What it solves

- No model training on your conversations
- Administrative controls
- Data retention policies
- Enterprise agreements (DPA, SSO)

What it does not solve

- It is still a general-purpose AI chat
- It doesn't understand your firm's workflow
- It doesn't enforce legal review processes
- It doesn't capture your firm's institutional knowledge

Legal AI Platforms

AI in Legal Practice: Maturity Levels

Maturity
Level

LEVEL
1



Consumer AI

(ChatGPT, Claude, Gemini)

General-purpose tools for individual use.
Not designed for legal practice.

LEVEL
2



Enterprise AI

(ChatGPT Enterprise, Claude Enterprise)

Stronger security, privacy, and admin controls for the organization.

LEVEL
3



Legal AI Platforms

(Harvey, Legora, CoCounsel)

Purpose-built for legal work with domain expertise and workflow tools.



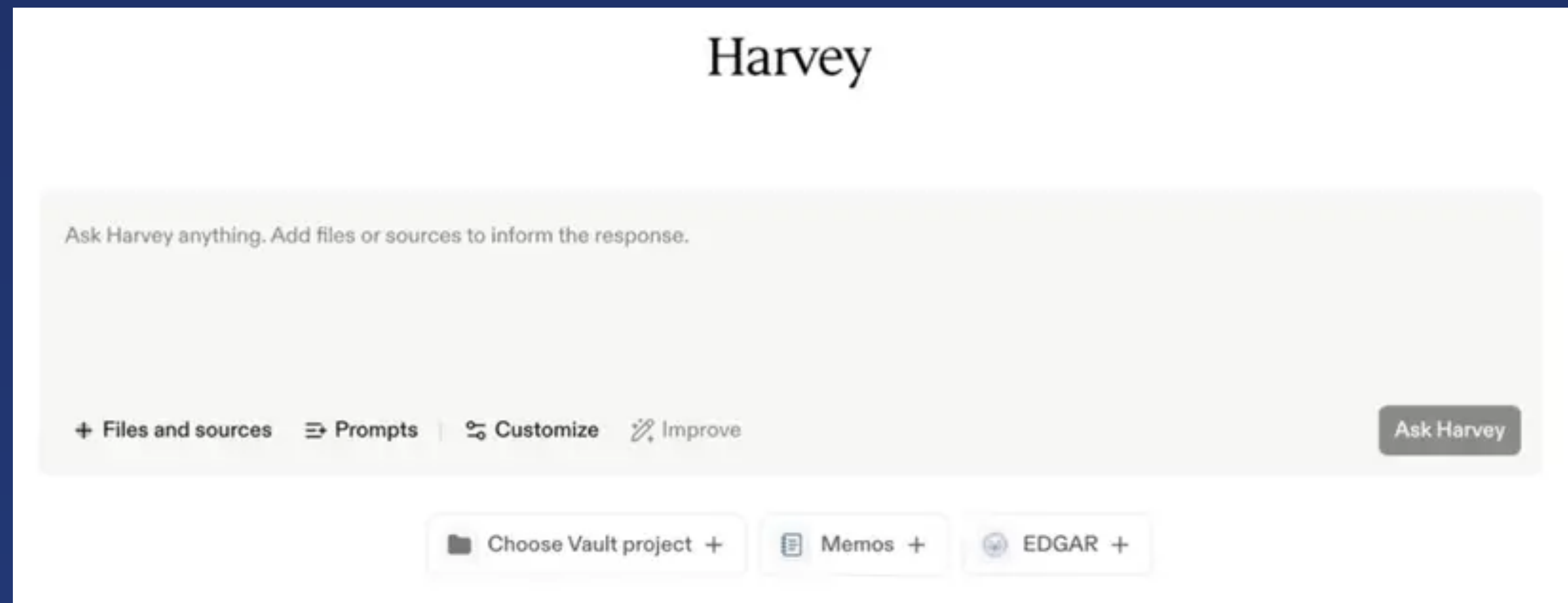
Firm-specific AI (Custom)

Built around your firm's unique workflows, knowledge, and practices.

Legal AI Platform (Harvey, Legora, CoCounsel)

What it solves

- Purpose-built for lawyers
- Legal-specific data sources and tools
- Better legal research
- Support for standard and custom workflows



Firm-specific AI

AI in Legal Practice: Maturity Levels

Maturity
Level

LEVEL
1



Consumer AI

(ChatGPT, Claude, Gemini)

General-purpose tools for individual use.
Not designed for legal practice.

LEVEL
2



Enterprise AI

(ChatGPT Enterprise, Claude Enterprise)

Stronger security, privacy, and admin controls for the organization.

LEVEL
3



Legal AI Platforms

(Harvey, Legora, CoCounsel)

Purpose-built for legal work with domain expertise and workflow tools.



Firm-specific AI (Custom)

Built around your firm's unique workflows, knowledge, and practices.

Firm-specific AI (custom)

What it solves

- Complete control over the user experience
- Complete control over legal workflows
- Complete integration with firm systems
- Capture your firm's unique expertise

Firm-specific AI (custom)

When should you build firm specific AI?

When you want to maximize productivity by having complete control over the workflow.

Every law firm has a handful of high-value workflows that are central to how it practices law.

Those workflows deserve software designed specifically for them.

Every Firm Has Its Own Way of Practicing Law.

That is your competitive advantage.

Condemnor appraisal review

Initial case assessment

Hearing preparation Mediation

Trial chronology^{notebook}

Client update letters

This is the special sauce that you should focus on
automating.

Learn More and Next Steps

Should Lawyers Upload Confidential Client Information to AI?

AI Category	Recommendation
 Consumer AI (ChatGPT, Claude, Gemini)	 No
 Enterprise AI	 Sometimes — if your firm's governance requirements are satisfied
 Legal AI Platforms (Harvey, Legora, CoCounsel)	 Yes — generally appropriate for professional legal work
 Firm-specific AI (Custom)	 Yes — when justified by the firm's most important workflows

**What's the one workflow you'd
automate first?**

Design your first AI workflow free.

StephenWalther.com