Introductions

Ken Button
Co-founder & CEO
ContractSafe

Ed Ortega
Partner
Machine & Partners

Nishat Ruiter
General Counsel
TED Conferences

Roadmap

1. From Novice to Know-It-All in 5 Minutes
2. How to Get What You Want from AI
3. AI Hacks for Everyday Tasks
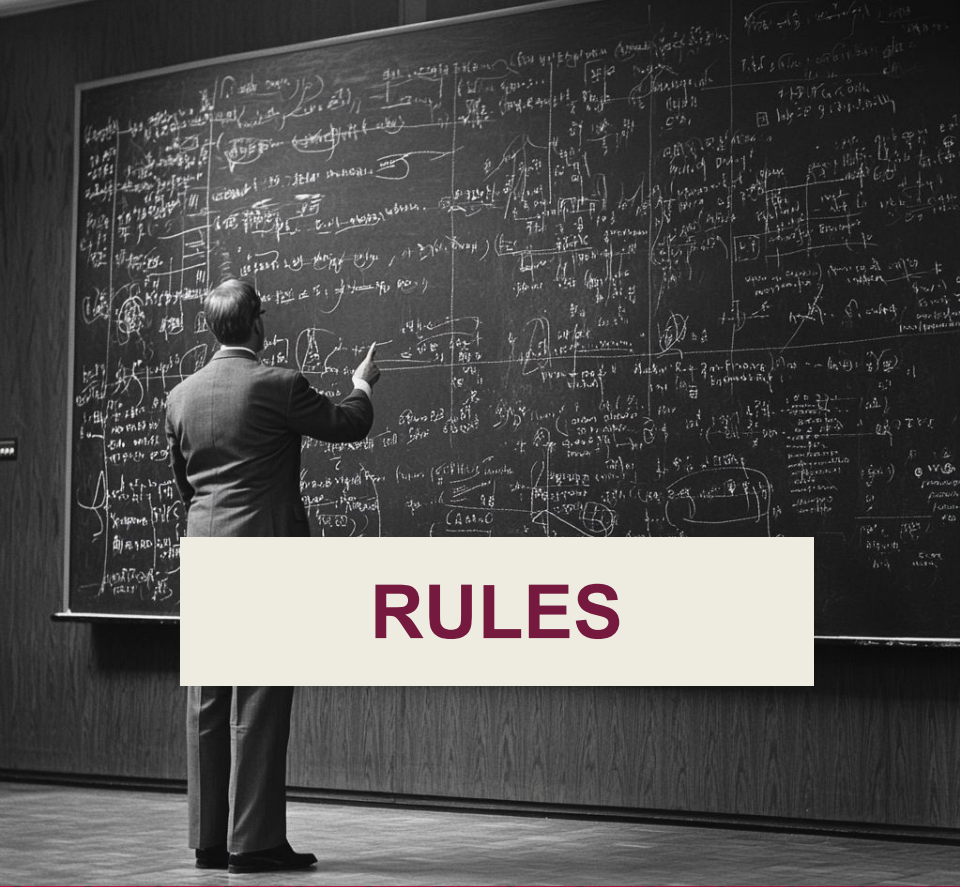4. Staying on the Right Side of the Law

AI 101:

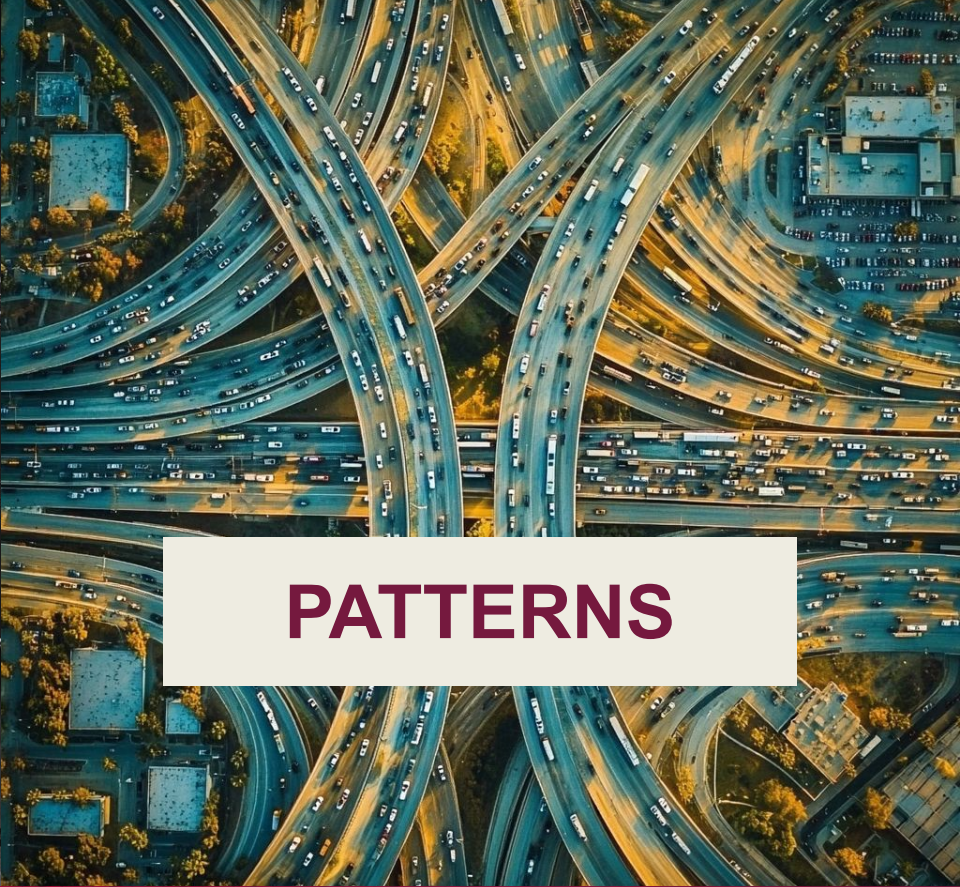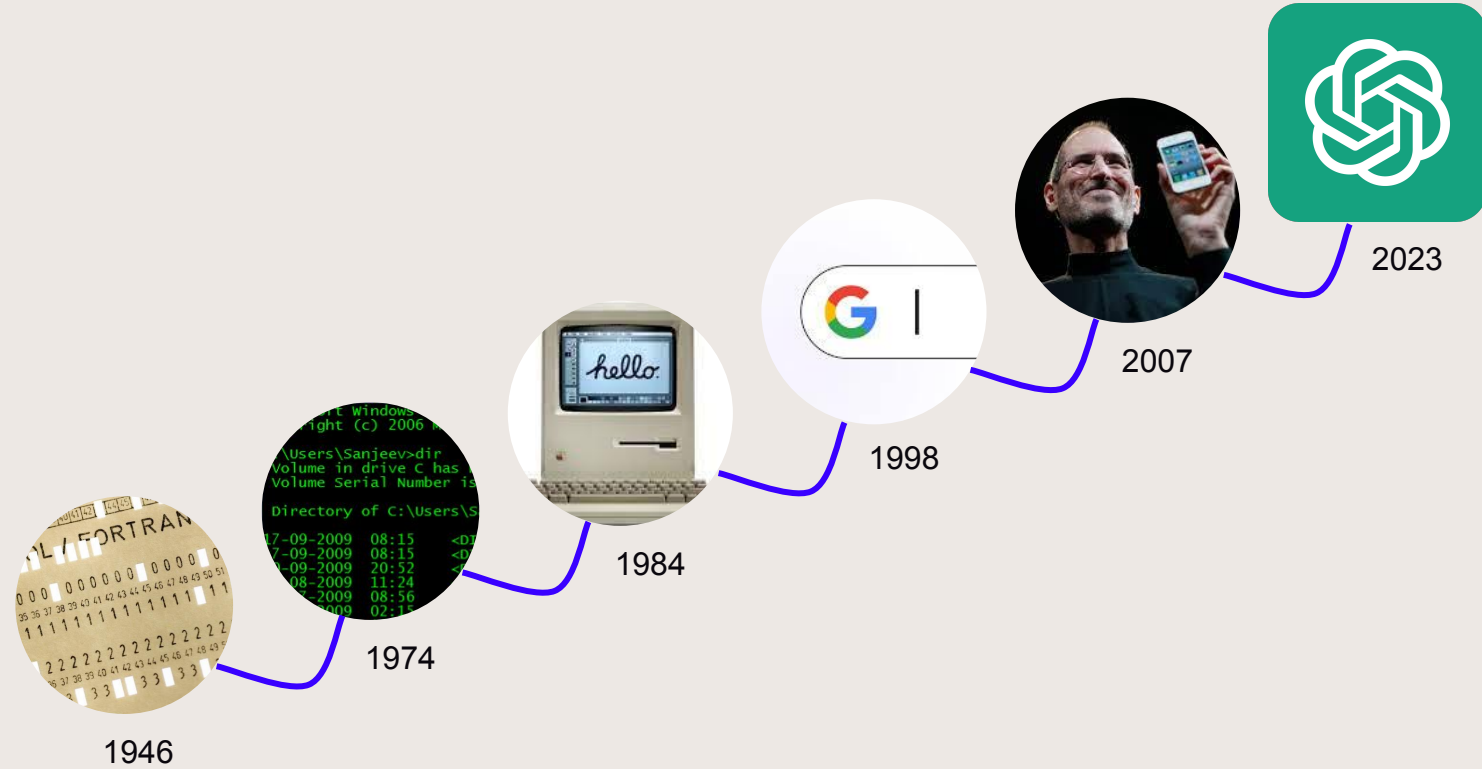# Everything You Need to Know About AI in 5 Minutes or Less

RULES

PATTERNS

GenAI

1946

1974

1984

1998

2007

2023

Garbage in, Garbage Out
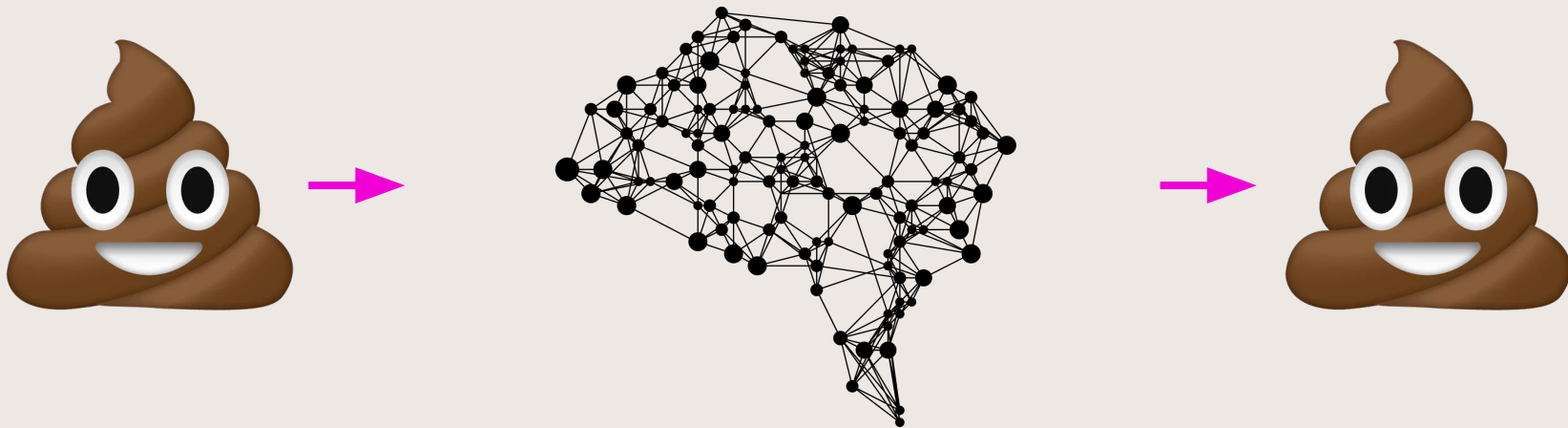
How to Get What You Want from AI

- **R** ole – Who is the AI embodying?
- **A** ction – What do you want the AI to do?
- **C** ontext – What does the AI need to know?
- **E** xamples – Can you give the AI an example?
- **R** estrictions – What are the limits or requirements for the AI?

Goodness In, Goodness Out

"You are a high school physics teacher. Explain the theory of relativity to me. But explain it to me as if I'm a freshman with limited knowledge of physics. Break it down into discrete concepts and explain each concept to me individually, stopping after each concept to ask if I understand before moving on to the next concept. Don't dumb down the concepts, but use everyday language instead of physics jargon when possible."

ChatGPT Protections

Total control over data and storage. As secure as your infrastructure.

Prompts, responses, and uploaded data can be used for QA purposes. Users can opt-out.

OpenAI commits to privacy, but data is stored in OpenAI's multi-tenant infra.

OpenAI model runs on Azure, data is encrypted & stored in single tenant.

Personal ChatGPT Account

Team/Enterprise ChatGPT Account

MS Azure OpenAI Service

Open Source Model on Private Hardware

4 Ways to Use AI Now

1. **Legal Research**
2. **NDA Hack**
3. **What the Judge said…**
4. **Charts for lawyers (!)**

Scope of using AI and legal implications

- Legal implications depend on the use
- Check that you have consent, met your privacy policy and not breaching your own terms.
- Check how the ABA guidance applies

Legal implications for using AI

Data Privacy – healthcare or finance data or misuse of personal data.

Intellectual Property – models use proprietary information without permission, question of ownership (copyright office).

Algorithmic Bias & Discrimination – particularly with biometric data used to determine outcomes.

Liability for AI decisions – high risk vs. low risk and impact when systems cause harm.

Transparency and Accountability – understanding the how especially for finance, healthcare and justice uses.

Employment Law impact based on automation disrupting workforce, ethics of cheap labor.

Evolving Regulations – such as EU AI Act, state laws, UNESCO, NIST etc.

Regulatory and Model rules that impact how we use AI

EU Artificial Intelligence Act

AI state regulations on ethics, transparency and responsible use

July 29, 2024

ABA issues first ethics guidance on a lawyer's use of AI tools

According to the EU Act

This regulation is the world's first comprehensive AI law, aiming to ensure safety, transparency, and respect for fundamental rights while fostering innovation in AI development across the EU.

Took effect on August 2024 – with the first major ban on unacceptable risk systems as of February 2025, with phased implementation through August 2026

The AI Act applies not only to companies based in the EU but also to any company that **places AI systems on the EU market** or whose AI-generated outputs are used in the EU. This means **U.S. companies** offering AI-driven products or services in the EU must comply with its regulations, even if they are not physically based there.

The Act categorizes AI systems by **risk levels** (unacceptable, high, limited, and minimal). Lawyers should advise clients on identifying which category their AI systems fall into. **High-risk systems**, like those used in healthcare or law enforcement, will require rigorous conformity assessments and ongoing oversight or may be banned.

U.S. companies deploying **generative AI** models (e.g., ChatGPT) in the EU must comply with transparency requirements, such as disclosing when content is AI-generated and ensuring that training data respects intellectual property rights.

Companies that violate its provisions face €35 million or 7% of global annual turnover

This applies to serious violations, particularly for prohibited AI applications.

1. An AI system that deploys subliminal techniques beyond a person's consciousness or purposely manipulative or deceptive to materially distort the behavior of a person or group that impairs their ability to make an informed decision. "AI driven toys that manipulate"

2. Criminal profiling used to assess a personality trait or characteristic.

3. Use of scraping accessing facial data from CCTV or internet.

4. Or an AI system that exploits the vulnerabilities of a person or group due to their age, disability or specific social or economic situation. – "Social scoring systems"

5. Some exceptions are made for law enforcement purposes, such as searching for missing persons or preventing terrorist attacks.

State laws regarding AI

focuses on privacy, bias, transparency, and consumer protection [According to NCSL, 45 states introduced AI bills, and 31 states have adopted resolutions regarding AI].

California has led the way with bills requiring transparency in AI training data and the use of AI in **political advertisements**. The state is also considering requiring developers to disclose how AI systems are trained and used, with a focus on consumer interactions and election integrity . Wisconsin has passed legislation that is similar.

Colorado and **Connecticut** have enacted laws targeting **high-risk AI systems**, particularly those used in decision-making for finance, healthcare, and employment. These laws mandate **impact assessments** and risk management protocols to prevent algorithmic bias, with regulators enforcing compliance.

New York's AI Bill of Rights, introduced in 2024, which aims to protect residents from harmful uses of AI by ensuring transparency, fairness, and accountability in AI systems.

Florida has introduced several legislative efforts to regulate the use of artificial intelligence (AI), focusing on transparency and the responsible use of AI in critical areas such as political advertising, privacy, and government decision-making.

Guidance issued by the ABA regarding AI tools

Formal Opinion 512, released in **July 2024** that refer to the Model Rules and guidance.

It applies to AI tools capable of generating new content like text, images, or videos, specifically focusing on **generative AI (GAI)**.

AI tools used in law may assist with tasks such as legal research, drafting documents, and predicting case outcomes

ABA Opinion 512 - released July 2024

Competence (Model Rule 1.1): Lawyers must have a **reasonable understanding of AI's capabilities and limitations.** They should verify AI-generated outputs to ensure accuracy, as reliance on AI without review could lead to providing inaccurate advice.

Confidentiality (Model Rule 1.6): Lawyers **must assess the risks of sharing client information** with AI tools, particularly self-learning systems. Informed client consent is necessary before using sensitive data with AI, especially when privacy might be compromised .

Communication (Model Rule 1.4): **Lawyers are required to disclose AI use if it influences significant decisions or impacts the basis of fees**. If AI is used for tasks such as evaluating legal strategies, lawyers must inform clients .

Supervisory Responsibilities (Model Rules 5.1 & 5.3): **Senior attorneys must oversee the use of AI** by subordinates, ensuring that confidentiality and security protocols are in place .

Reasonableness of Fees (Model Rule 1.5): **Lawyers should only charge clients for the actual** time spent using AI tools, especially if those tools expedite legal work.

EYELEVEL SERVICE

EyeLevel for Legal

EyeLevel Legal AI is your litigation co-pilot, helping you get fast answers before, during and after trial.

Talk to Us

Fugees rapper not helped by his lawyer using AI software

In the pending motion for new trial, Pras Michel argues that the **AI software**, and consequently his counsel**, botched the closing argument**. The AI-generated closing, says Michel, "ignor[ed] the best arguments and conflat[ed] the charge schemes" and "misattributed" certain relevant songs. The AI software created a closing argument that, allegedly, "was deficient, unhelpful, and a missed opportunity that prejudiced the defense." Michel argues, too, that his lawyer had an undisclosed financial interest given his investment in EyeLevel Legal AI.

Judge sanctioned 2 lawyers for citing fictitious cases

The original case involved a man suiting an airline over an alleged personal injury

His legal team (Levidow, Levidow & Oberman) submitted a brief that included six fictitious case citations generated by an artificial intelligence chatbot, ChatGPT.

The judge found the lawyers acted in bad faith and made "acts of conscious avoidance and false and misleading statements to the court." Fined the lawyers $5,000.

Lawyer who used it added that he "greatly regrets" relying on the chatbot, which he said he had never used for legal research before and was "unaware that its content could be false"

Q&A

Thank You!

AI Hacks Recap
Your Go-To Resource Hub