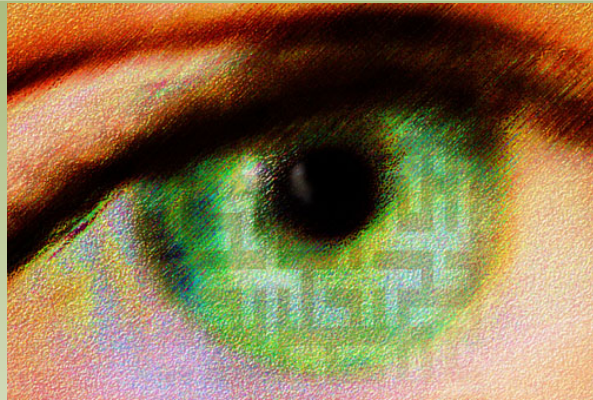# AI and the Practice of Law

Hennepin County Law Library

May 16, 2025

John J. Carney, Esq.

Carney Forensics

My History of AI

MIT AI Lab / Media Lab

Natural Language and Machine Vision

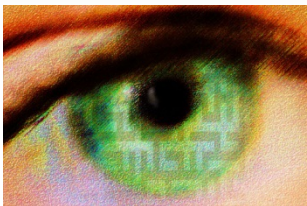| Symbolic AI	vs.	Deep Learning
		Machine Learning
Rules-based, Expert systems		Connections-based, Neural Nets
CPUs		GPUs
Minsky and Papert		McCullough and Pitts

GPTs and LLMs

GPT – Generative Pre-trained Transformers
LLM – Large Language Model (Machine Learning)

- Generative AI Tools Create Text, Images, Video, Music, Animations
- Draft Documents, Books, Poems, Software, Websites
- Summarize, Research, Translate, etc.
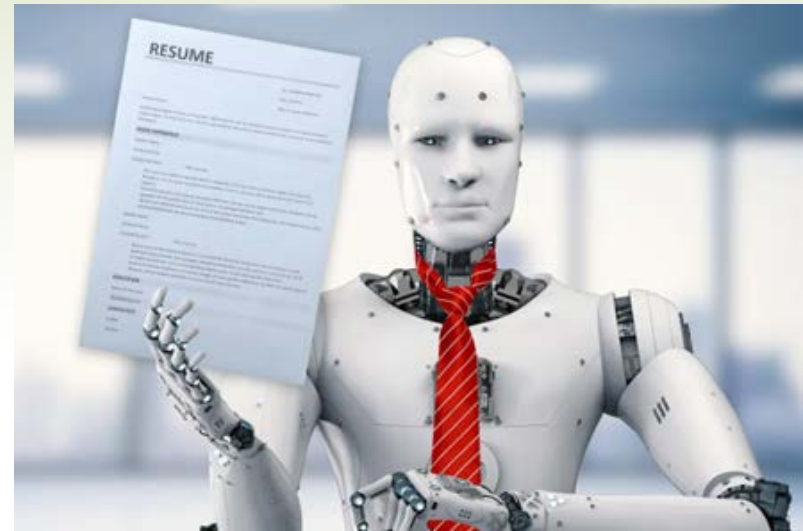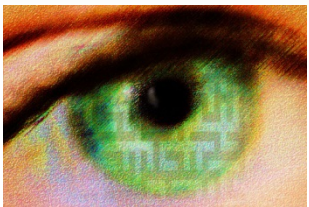
Modern History – November 2022

Generative AI based on Machine Learning and LLMs

OpenAI ChatGPT 3.5, 4.0, 4.1, 4.5

Microsoft CoPilot
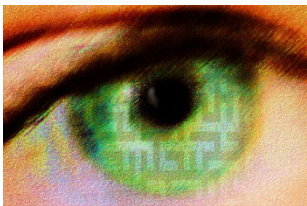
Google (DeepMind) Gemini 2.5

Anthropic Claude 3.7 Sonnet

Meta Llama 4

Perplexity (ChatGPT, Claude, Llama, Grok)
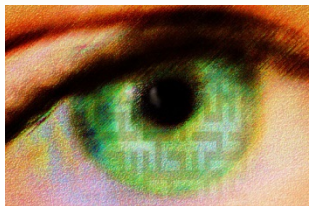
DeepSeek R1 (Open Source from China)

ChatGPT Takes the Lead

GPT 4's Uniform Bar Exam Performance

GPT 3.5   10% Pass Rate
GPT 4.0   90% Pass Rate (February – Repeaters)
GPT 4.0   68% Pass Rate (July – First Timers)

Legal AI Examples

Draft Answer to Complaint/Pleading
- Gen AI Tool Reviews Case Complaint
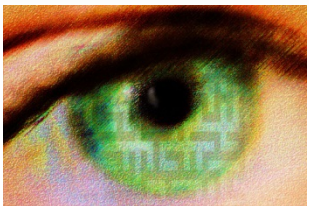- Prompt AI to Generate Multiple Answers

Damien Riehl

Draft Counter Arguments to Motion to Dismiss
- Prompt AI for Bulleted List of Counter Arguments
- Prompt AI for Sub-Bullets for Elements of Claims

Predict Litigation Outcomes from Court Case Stats
- Court Jurisdiction, Judge, Case Type
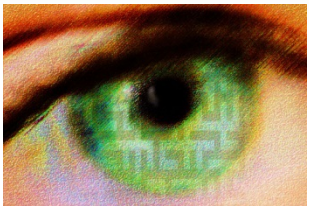- Stage of Litigation Lifecycle

Headlines

"Generative AI could radically alter the practice of law"

"Even if it doesn't replace lawyers en masse"

Security & Legal Ethics

Four Basic ABA Model Rules that Govern

Rule 1.1 **Competence** ⟵

Rule 1.4 Communications

Rule 1.6 Duty of **Confidentiality** ⟵

Rule 5.1, 5.2, 5.3 Lawyer & Nonlawyer Associations

The **"Big Two"** in Network or Cybersecurity

Begin Your Journey Toward **Competence** to Keep *Office* Data, Documents, and Communication **Confidential**

40 States Have Adopted Revised Rule 1.1
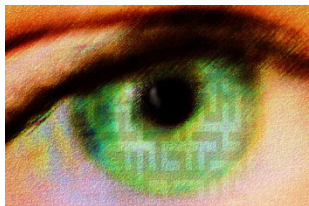
"To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*"

AI & Legal Ethics

AMERICAN BAR ASSOCIATION
STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 512   **July 29, 2024**
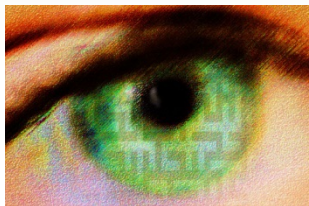
Generative Artificial Intelligence Tools

To ensure clients are protected, lawyers using generative artificial intelligence tools must fully consider their applicable ethical obligations, including their duties to provide competent legal representation, to protect client information, to communicate with clients, to supervise their employees and agents, to advance only meritorious claims and contentions, to ensure candor toward the tribunal, and to charge reasonable fees.

I.   Introduction

Many lawyers use artificial intelligence (AI) based technologies in their practices to improve the efficiency and quality of legal services to clients.[1] A well-known use is electronic discovery in litigation, in which lawyers use technology-assisted review to categorize vast quantities of documents as responsive or non-responsive and to segregate privileged documents. Another common use is contract analytics, which lawyers use to conduct due diligence in connection with mergers and acquisitions and large corporate transactions. In the realm of analytics, AI also can help lawyers predict how judges might rule on a legal question based on data about the judge's rulings; discover the summary judgment grant rate for every federal district judge; or evaluate how parties and lawyers may behave in current litigation based on their past conduct in similar litigation. And for basic legal research, AI may enhance lawyers' search results.

This opinion discusses a subset of AI technology that has more recently drawn the attention of the legal profession and the world at large – generative AI (GAI), which can create various types of new content, including text, images, audio, video, and software code in response to a user's prompts and questions.[2] GAI tools that produce new text are prediction tools that generate a statistically probable output when prompted. To accomplish this, these tools analyze large amounts of digital text culled from the internet or proprietary data sources. Some GAI tools are described as "self-learning," meaning they will learn from themselves as they cull more data. GAI tools may assist lawyers in tasks such as legal research, contract review, due diligence, document review, regulatory compliance, and drafting letters, contracts, briefs, and other legal documents.

Steven Schwartz & Peter LoDuca

NEW YORK, June 22 (Reuters) - A U.S. judge on Thursday imposed sanctions on two New York lawyers who submitted a legal brief that included six fictitious case citations generated by an artificial intelligence chatbot, ChatGPT.

U.S. District Judge P. Kevin Castel in Manhattan ordered lawyers Steven Schwartz, Peter LoDuca and their law firm Levidow, Levidow & Oberman to pay a $5,000 fine in total.

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

Levidow, Levidow & Oberman said in a statement on Thursday that its lawyers "respectfully" disagreed with the court that they acted in bad faith.

"We made a good faith mistake in failing to believe that a piece of technology could be making up cases out of whole cloth," the firm's statement said.
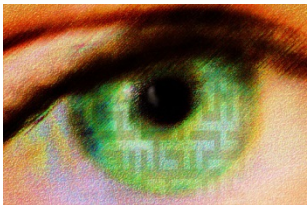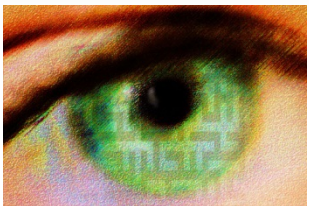
Steven Schwartz

Steven Schwartz – NY Personal Injury Lawyer
Drafted court filing relying on AI chatbot ChatGPT
Motion had <u>made-up</u> cases, rulings and quotes
Lawyer filed motion after ChatGPT assured him:
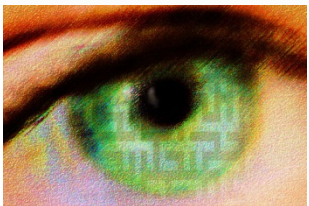 "The cases I provided are real and can be
found in reputable legal databases"

(They were not, and can not)

Canadian lawyer Chong Ke

Turned to ChatGPT when her client wanted to know if he could take his children on an overseas trip in the midst of a custody dispute.

To make her argument, Ke cited precedent from two court cases that ChatGPT had supplied—both of which were completely made up.

When it was all said and done, Ke had to pay the court costs it took for the opposing counsel to research the nonexistent cases.

Caveat Emptor – Due Diligence

Falsehoods, Lies -> AI Hallucinations

AI LLMs are trained on:

Entire Internet, books, magazines, blogs, etc.

Also, legal documents and evidence

AI generates language based on lawyers' prompts

But, crucially, does not Shepardize it!

Lawyer's obligation to Shepardize, KeyCite, etc.

Check your citations!!
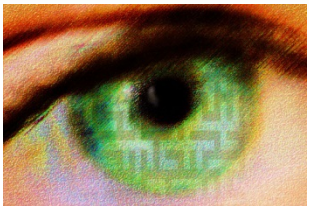
Caveat Emptor – Hallucinations

ChatGPT Hallucinations are Falsehoods / Lies

- AI States them with Unusual Confidence
- LLM is Trained on Internet Content and More

- OpenAI: "ChatGPT may produce inaccurate information about people, places, or facts."

- Google: "Bard (Now Gemini) may display inaccurate information or offensive statements."
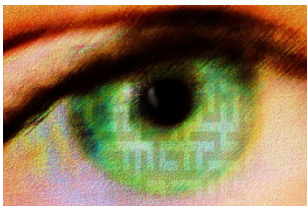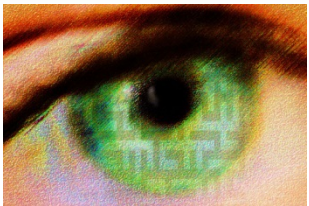
Expert Prompt Engineer's Advice

Large Language Models:

Sometimes Wrong

Never in Doubt

Always Confident

Never Say, "I Don't Know"

AI Confidentiality & Security

Public documents are safe

    Statutes, Rules, Regs, Published Opinions

Gen AI exposes sensitive, privileged client data by sharing with LLMs to train

    Oversharing and over-permission accounts

    Exposes prompts that guide AI tool

    Exposes legal documents uploaded to AI tool

Confidentiality breaches of ACP and WPD and NDAs
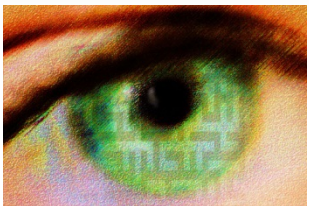
AI Confidentiality & Security

Know your AI Tool

Choose AI legal drafting tools carefully

    Confidentiality

    No sharing with LLM training data

    Examples

        Westlaw AI-Assisted Research

        Westlaw Quick Check

        Casetext CoCounsel
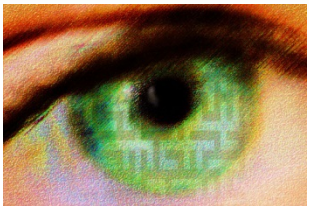
        vLex Vincent AI
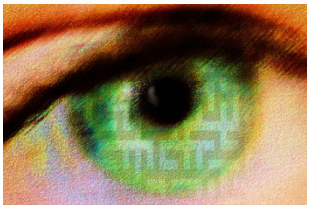
AI Confidentiality & Security

Perform due diligence on AI tools' third parties

And their partners

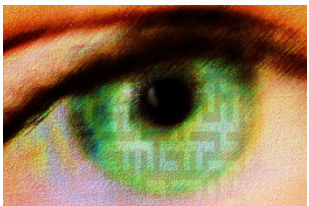   Trust, but verify

      Perform audits
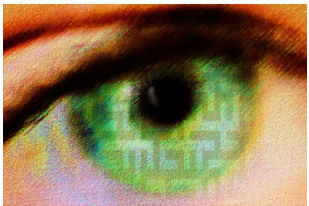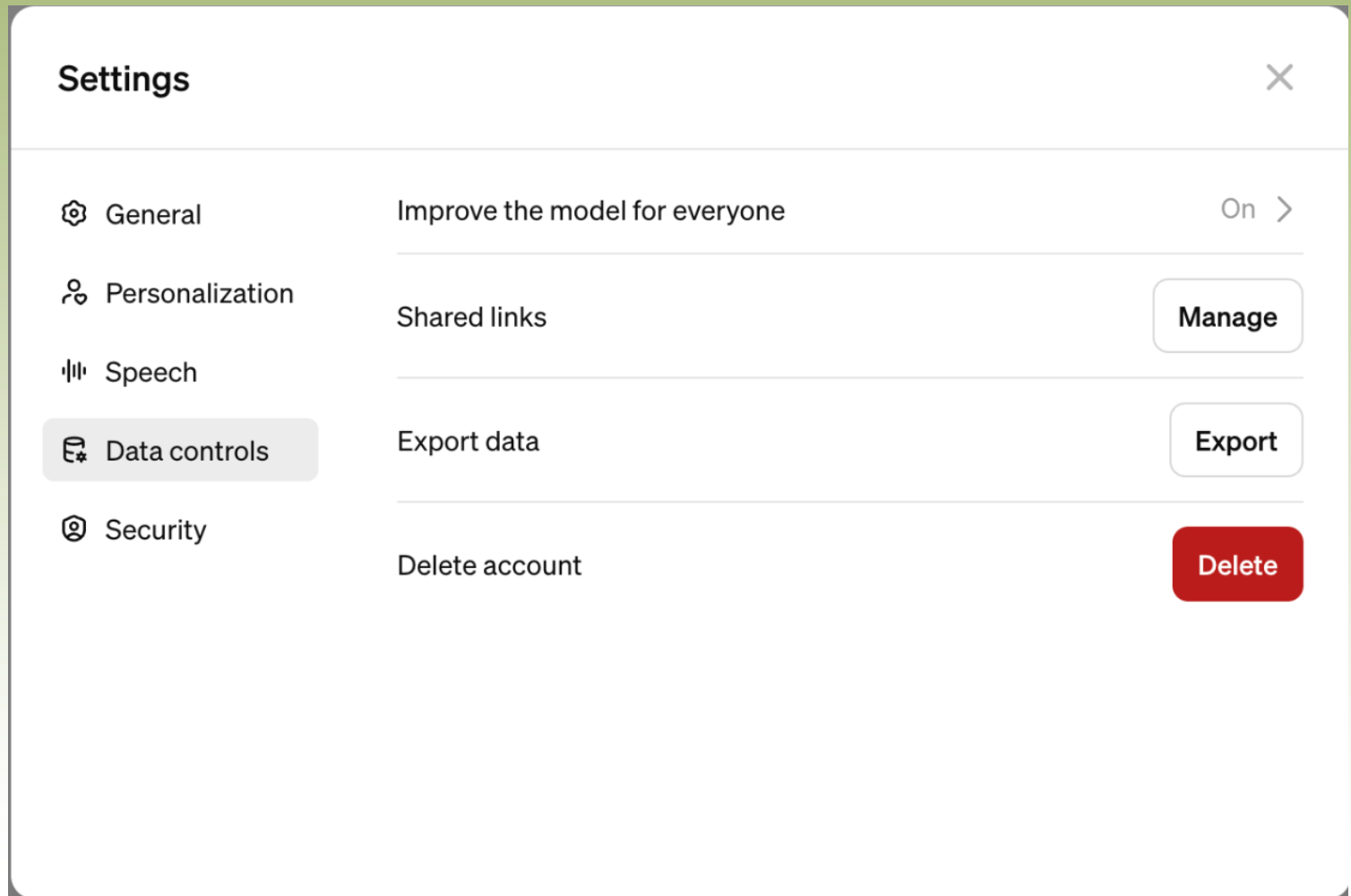
      Contracts with third parties and their partners

AI Confidentiality

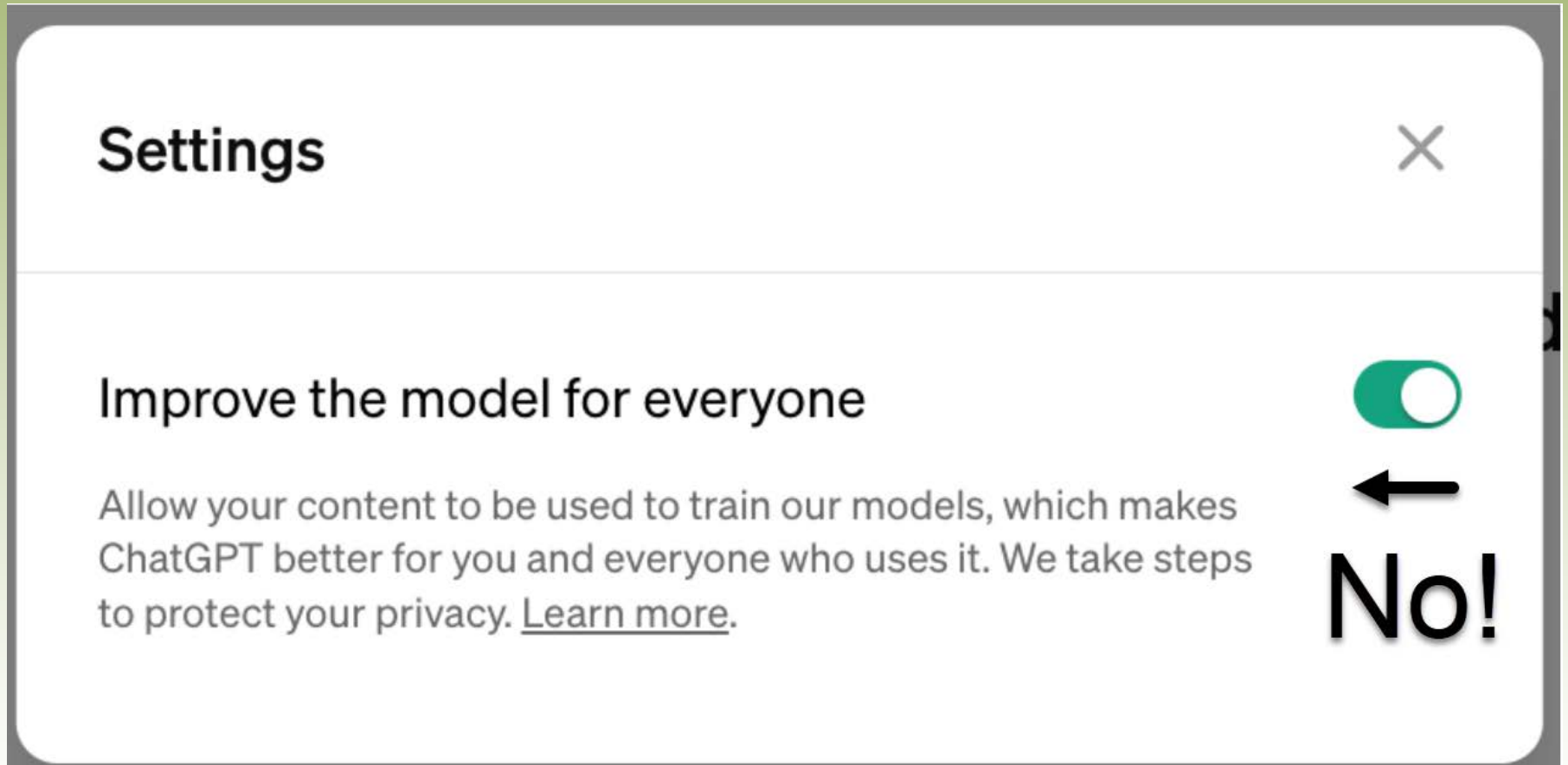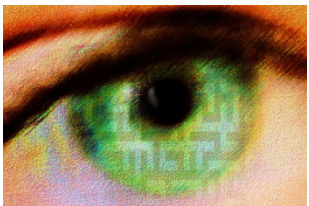Opt out of sharing training data with LLMs (e.g. ChatGPT, Gemini, Claude)

Eliminate data leakage

ChatGPT Confidentiality

Settings   ✕

⚙ General	Improve the model for everyone On ›
👥 Personalization	Shared links **Manage**
⍦ Speech	
🗄 Data controls	Export data **Export**
◉ Security	Delete account **Delete**

ChatGPT Confidentiality

Settings ✕

Improve the model for everyone

Allow your content to be used to train our models, which makes ChatGPT better for you and everyone who uses it. We take steps to protect your privacy. Learn more.

← No!

Gemini Confidentiality

Google Workspace Admin Help

🔍 Describe your issue

**Business / Enterprise**   Education

What is the Gemini app?   ˅

Who can use the Gemini app?   ˅

What if I don't have Google Workspace today? What if I don't have the right edition?   ˅

How does Gemini for Google Workspace protect my data?   ^

When Google Workspace commercial customers adopt Gemini for Google Workspace, they get the same robust data protection and security standards that come with all Google Workspace services, with specific protections for businesses, education, and public-sector customers:

- Users with a Gemini for Google Workspace license get enterprise-grade data protections when they use Gemini app. ==Submissions aren't used to train models== and are never reviewed by humans. Learn more about how Gemini app works for users who don't have a license.
- Your interactions with Gemini for Google Workspace stay within your organization. ==Gemini for Google Workspace stores any prompts or generated content== alongside your Workspace content and ==does not share them outside your organization.==
- Your existing Google Workspace protections are automatically applied. Gemini for Google Workspace brings the same enterprise-grade security as the rest of Google Workspace, automatically applying your organization's existing controls and data handling practices, such as data-regions policies and Data Loss Prevention.
- Your content is not used for any other customers. ==None of your content is used for model training outside of your domain without permission.==
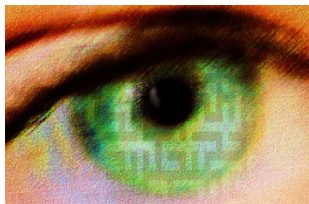
Gemini Confidentiality

Gemini app

Users ∨

Groups ∨

Organizational Units ∨

Showing settings for users in **Test Org**

Gemini conversation history

Gemini conversation history
Applied at 'Test Org'

Gemini conversation history controls allow admins to control if conversations with Gemini are saved and for how long before they are automatically deleted. Disabling Gemini conversation history will not affect previous conversation history which is subject to the auto-delete setting below.

Gemini conversation history
Gemini conversation history allows users to return to past conversations

☑ Enable Gemini conversation history
Uncheck to turn Gemini history off

Conversation retention
Choose when conversations should be deleted from a user's history

18 months ▾
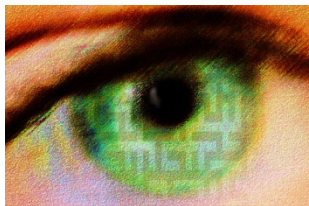
AI Confidentiality

Opt out of each LLM for AI Tools that use multiple LLMs (e.g. Perplexity)

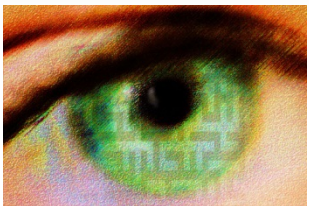Eliminate data leakage
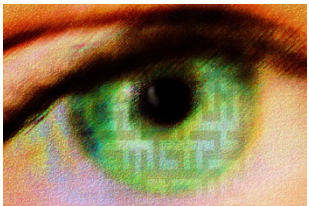
Perplexity Confidentiality
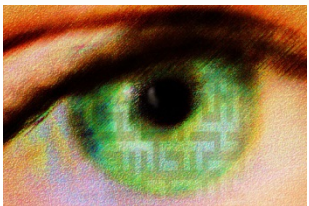
AI Confidentiality

Use Professional / Paid version of AI Tool

Not free version (Lawyer as product)

Pro / Paid version has settings
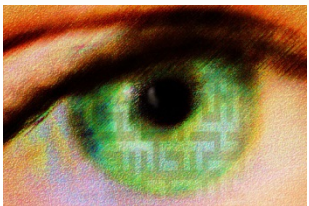
Settings for opting out of LLMs

AI Security

Apply modern cybersecurity practices

Strong Credentials

Complex passcode, not reused

Apply 2FA protection to AI account

Use encryption for prompts, uploaded documents, AI threads

ChatGPT Security
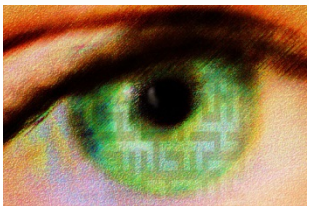
Two-Factor Authentication (2FA)

- It's a 2nd, Time-based Password for Secure Access to Web Accounts and Mobile Apps
- It's Something You "Know", "Possess", or "Are"
  - "Know" Your Passwords, Pass Phrases, and PINs
  - "Possess" Your Smart Phone for Confirmation from Authenticator Apps
  - "Possess" Your YubiKey (USB Security Key) for Convenient Authentication
 - You "Are" Your Biometric Fingerprint, Face Scan, Retina Scan
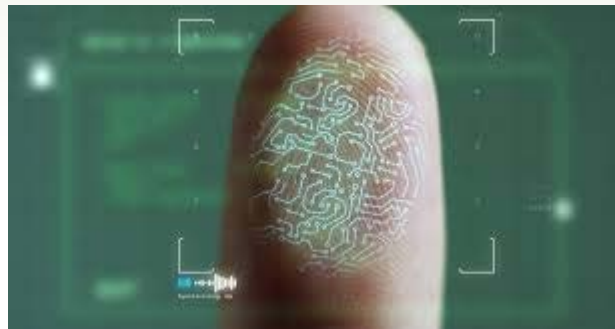
Two-Factor Authentication (2FA)

- Google says 2FA Blocks Attacks
  - "We found that an SMS code sent to a recovery phone number helped block 100% of automated bots, 96% of bulk phishing attacks, and 76% of targeted attacks. On-device prompts, a more secure replacement for SMS, helped prevent 100% of automated bots, 99% of bulk phishing attacks and 90% of targeted attacks."
- Microsoft says 2FA Blocks 99% of Attacks
- You Need 2FA When Working on AI
  - ChatGPT, Gemini, Claude, etc.
    - Load Google Authenticator on Your Smart Phone
    - Bring Your YubiKey (USB Security Key) Home
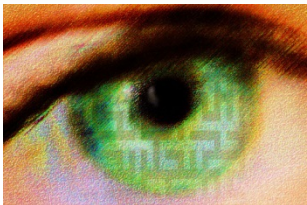
Caveat Emptor – Plagiarism

ChatGPT Draws from LLM including Internet

Plagiarism -> Academia

Give credit, attributions, cite everything

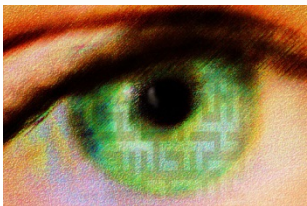Detector Tools for Plagiarism / AI Generated Content

Some better than others

Some hard to use correctly

Tools to try:

Copyleaks
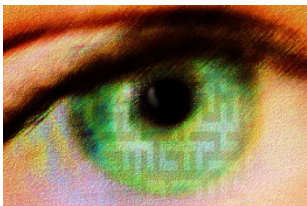
Originality.ai

Caveat Emptor – Copyright

ChatGPT Draws from LLM including Internet
Copyright ->Infringement, but...

Ideas can't be copyrighted

Facts can't be copyrighted

Expressions can be copyrighted, but machine expressions cannot

Small Language Models (SLM)

SLM as an alternative to LLMs

MIT Technology Review 2025 Breakthrough

"For certain tasks, smaller models that are trained on more focused data sets can now perform just as well as larger ones—if not better. That's a boon for businesses eager to deploy AI in a handful of specific ways. You don't need the entire internet in your model if you're making the same kind of request again and again."
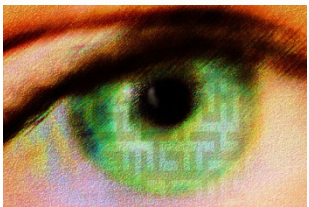
Small Language Models (SLM)

SLM as an alternative to LLMs

Legal Applications

Firm Brief Bank

MACDL, MAJ, MDLA Brief Banks

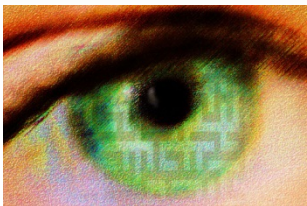All Firm's Practice Area Brief Bank

All Firm's Brief Banks (public)

Orders in all courts

in this court

from this judge

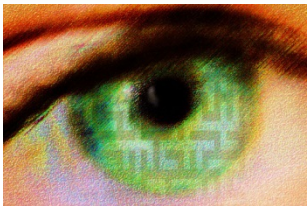All Legal Documents in my case

Electronic Discovery in my case

What about Your Experts?

Digital Evidence and Testimony is Changing Too

AI Machine Vision
AI Natural Language
Digital Forensics

Expert Witness – Prof. Jeff Hancock

Stanford Communications Prof. Jeff Hancock filed an expert report supporting Minnesota's law, but that report did not go well. Prof. Hancock used Generative AI to help draft the report. The Generative AI hallucinated citations (as it is known to do), and he didn't catch the fake citations.

As a result, he submitted an erroneous expert report.
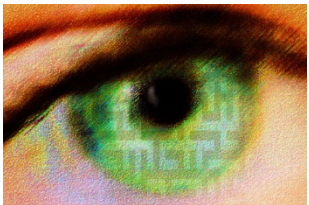
Expert Witness – Prof. Jeff Hancock

"The irony. Professor Hancock, a credentialed expert on the dangers of AI and misinformation, has fallen victim to the siren call of relying too heavily on AI—in a case that revolves around the dangers of AI, no less."

"The Court thus adds its voice to a growing chorus of courts around the country declaring the same message: verify AI-generated content in legal submissions!"
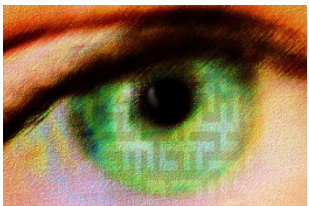
Expert Witness – Charles Ranson

Trusts & Estates Litigation Consultant & Expert Witness

Used Microsoft CoPilot to generate computations

Straightforward rate of compound return

   Theoretical value of reinvested proceeds from mutual fund

   Do not need AI or an expert to calculate it

AI improvises answers which vary each time it's calculated

Not repeatable and calls into question the reliability and accuracy of the AI

Evidence considered unreliable, inaccurate, and inadmissible at court

Court wanted to see a disclosure of use of AI to generate evidence

      Court also wanted to see AI generated evidence subject to

      a Frye hearing before admission
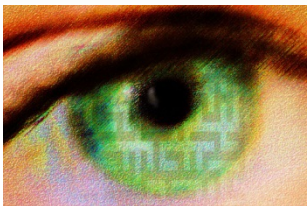
AI Natural Language Processing

Chat Thread Categorizations

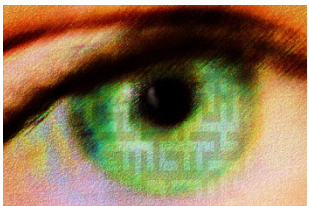   Grooming, Luring

    Sex-Related

Chat Threads – Ask Questions of AI Agent

    Artifacts in Magnet CoPilot

Web Searches – Ask Questions of AI Agent

    Artifacts in Magnet CoPilot

AI to Recover Digital Evidence

AI Vision and Auto-Tagging (Machine Vision)

Recognize/Categorize Thousands of Photos and Videos
- Documents, ID/Credit Cards, Invoices/Receipts
- Money, Weapons, Nudity, Human Hands, Drugs
- QR/Barcodes, Handwriting, Icons, Hate Symbols
- Drones, Vehicles, Aircraft, License Plates
- Militants, Tattoos, Buildings, Bedrooms

Recognize Smartphone Screenshots – Recover
Forgotten, Now Deleted, Text Messages,
Chat Threads, Emails, Posts
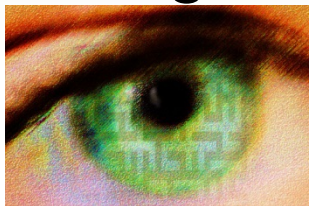
AI to Recover Digital Evidence

AI Vision and Auto-Identity and Search

- Forensic Reverse Image Search
  - Similar to Google reverse image search
  - Samples of target person provided by party
  - AI locates matches from the device revealing legally forbidden relationships
- OCR (Optical Character Recognition)
  - Process entire device for photos, videos, unsearchable PDFs
  - Search keyword lists for relevant matches
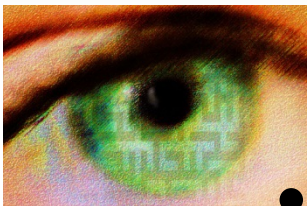
AI to Recover Digital Evidence

AI Vision and Auto-Identity and Search

- Photo and Video Enhancement
  - Fix Blurry Quality
  - Clarification and legibility for traffic lights, license plates, train yards, etc.
- Photo and Video Authentication
  - Detect Tampering
  - Detect Deepfakes and Synthetic Media
  - Recognize AI Generation of Media
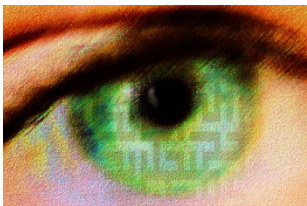
Future of AI Digital Forensics

AI summarizes messages, emails, documents, notes, web searches

AI automatically generates evidence timelines for a date range

AI automatically generates GPS maps for selected artifacts or date range

AI filtering based on Trial Lawyers' goal of examination

AI device identification from audio recordings of smartphone make and model from recorded audio specimen
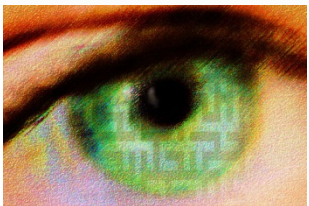
AI identification of smartphone knock-offs
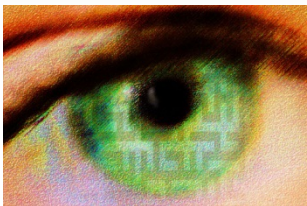
AI identification of audio splicing with exact locations of fraudulent splices

What Are AI "Deepfakes"?

What is a "Deepfake"?

The court explains:

> Deepfakes are image, audio, or video files that mimic real or nonexistent people saying and doing things that never happened. Deepfakes leverage artificial intelligence ("AI") algorithms to manipulate digital content—ordinarily images, sounds, and videos—in which a person's likeness, voice, or actions are convincingly altered or fabricated. The AI technology behind deepfakes is advanced and complex, making it difficult for the average person to detect the falsity of a deepfake.

Proposed AI Amendments to
# Federal Rules of Evidence

In response to serious problems of abuse of generative AI in creating digital evidence for jurisprudence

U.S. Judicial Conference Advisory Committee on Evidence Rules

Rule 901 - AI Authentication of language (text) and media (video, photo, audio) modalities

Rule 901(c) - Identification of deepfakes and AI alterations which shift the burden of proof

Rule 707 - Role of Digital Forensic Experts as AI Authenticators
      to satisfy Rule 702 criteria
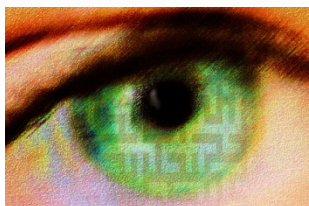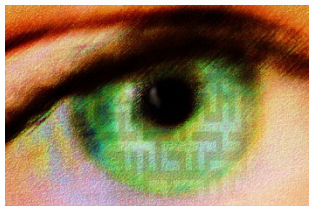
AI is Tool in Its Infancy

Neither Fad nor Apocalypse
Will Radically Change:

- How Lawyers Work and Law Firms Make Money

Legal
Profession:

- Unabashedly Clear AI Use Case
- With Sky High Risk
- Get It Right and Reap Rewards
- Laggards Risk Going Way of Typesetters

Questions & Answers

Carney Forensics

"Digital Evidence is Everywhere"

Cell Phones / Smart Phones

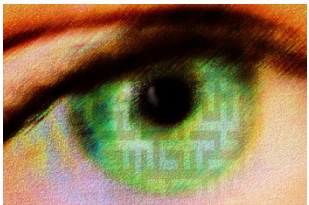**Smart Tablets**

Computer Forensics

GPS Devices

Social Media / Web Mail

Sign up for our Newsletter!!
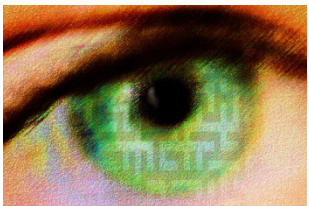
www.carneyforensics.com

Caveat Emptor - Hallucinations

ChatGPT Hallucinations are Falsehoods / Lies

- Lawyers Must Choose AI Tools Trained On:
  - Reputable Legal Databases / Documents
  - From Lawyer's Practice Area / Jurisdiction

- Lawyers Can Train AI on Law Firm's Documents
  - Lawyers Must Prompt AI Effectively to Reduce Hallucinations

Caveat Emptor - Confidentiality

Lawyer's ChatGPT Prompts Are Not Private

- Attorney Client Privilege Issues
- Work Product Doctrine Issues
- Other Non-Disclosure Issues

- Lawyers Must Choose AI Tools:
  - Protect Legal Prompts and Instructions
  - Ensure They Are Separate and Apart from Shared and Public Data