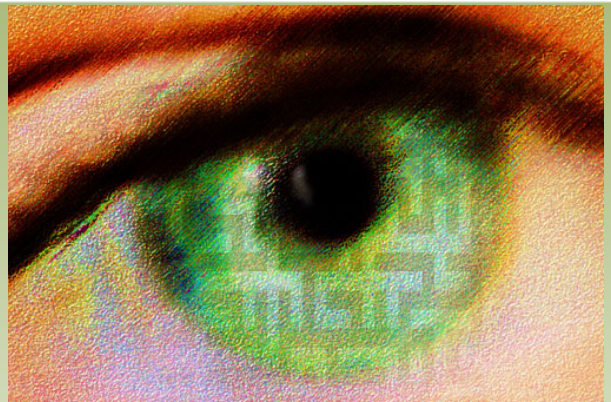
AI and the Practice of Law

Minnesota State Law Library

October 23, 2025

John J. Carney, Esq.

Carney Forensics



My History of AI

MIT AI Lab / Media Lab

Natural Language and Machine Vision

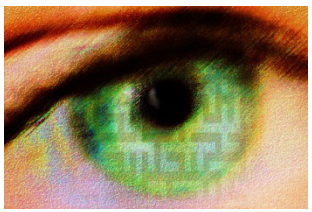
Symbolic AI	vs.	Deep Learning
		Machine Learning
Rules-based, Expert systems		Connections-based, Neural Nets
CPUs		GPUs
Minsky and Papert		McCullough and Pitts

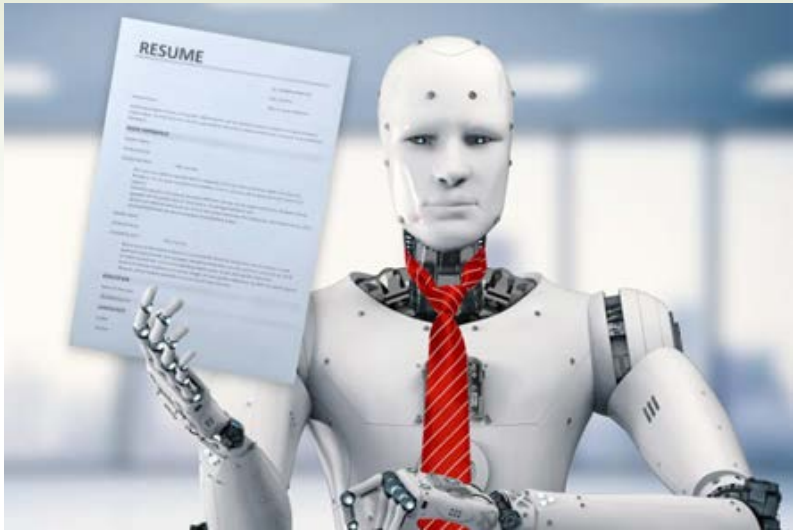
Prof. Patrick Winston

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, 5.0

Microsoft CoPilot

Google (DeepMind) Gemini 2.5

Anthropic Claude 4.5 Sonnet

Meta Llama 4

Perplexity (ChatGPT, Claude, Llama, Grok)

DeepSeek V3 (Open Source from China)

ChatGPT Takes the Lead

Massachusetts Institute of Technology

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

Damien Riehl

Draft Answer to Complaint/Pleading

- Gen AI Tool Reviews Case Complaint
- Prompt AI to Generate Multiple Answers

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

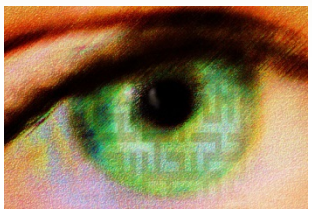
- Court Jurisdiction, Judge, Case Type
- Stage of Litigation Lifecycle

Headlines

The Economist

“Generative AI could radically alter the practice of law”

“Even if it doesn’t replace lawyers en masse”



Security & Legal Ethics

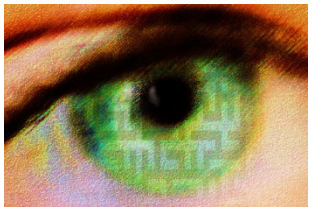
Four Basic ABA Model Rules that Govern

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

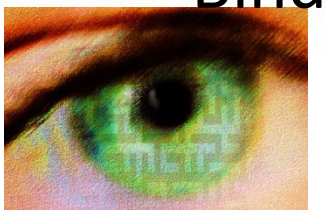
To ensure clients are protected, lawyers using generative artificial intelligence tools must fully consider their applicable ethical obligations, including their duties to provide competent legal representation, to protect client information, to communicate with clients, to supervise their employees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

AI Contract Compliance

"No Confidential Information may be uploaded to, processed by, or disclosed to any publicly available AI/ML system, model, or dataset without prior written consent."

AI-specific clauses are starting to appear in contracts as legal teams and AI law specialists are recommending clauses that:

- Ban feeding confidential data into public models without written consent
- Require proof that approved tools will not train on data
- Bind contractors and sub-processors to same rules



Steven Schwartz

The Economist

Steven Schwartz – NY Personal Injury Lawyer
Drafted court filing relying on AI chatbot ChatGPT
Motion had made-up 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)

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.

Caveat Emptor – Due Diligence

Falsehoods, Lies -> AI Hallucinations

AI Foundation 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!!

Noland v. Land of the Free, L.P.

California Court of Appeals

First case to explicitly address opposing counsel's role in detecting AI hallucinations

Plaintiff used AI tools to enhance appellate briefs

21 of 23 case citations were fabricated, failed to check them

No sanctions ordered for attorney fees for opposing counsel

Respondents did not alert court to fabricated citations

Case hints at evolving standard of professional competence

Expert Prompt Engineer's Advice

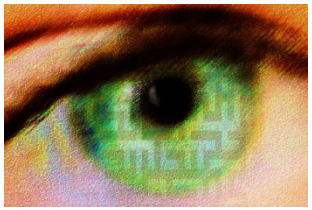
Large Language Models:

Sometimes Wrong

Never in Doubt

Always Confident

Never Say, "I Don't Know"



AI Confidentiality & Security

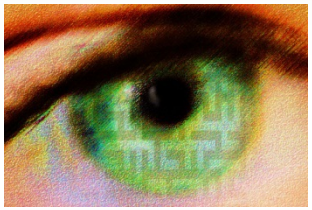
Public Documents are Safe

- Statutes, Rules, Regs, Published Opinions

Generative AI Exposes Sensitive, Privileged, Client Data by Sharing with LLMs to Train

- Exposes User Prompts that Guide AI Tool
- Exposes Legal Documents Uploaded to AI Tool
- Too Much Account Access via Permissions

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
  - Lexis + AI
  - BriefCatch
  - Harvey

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

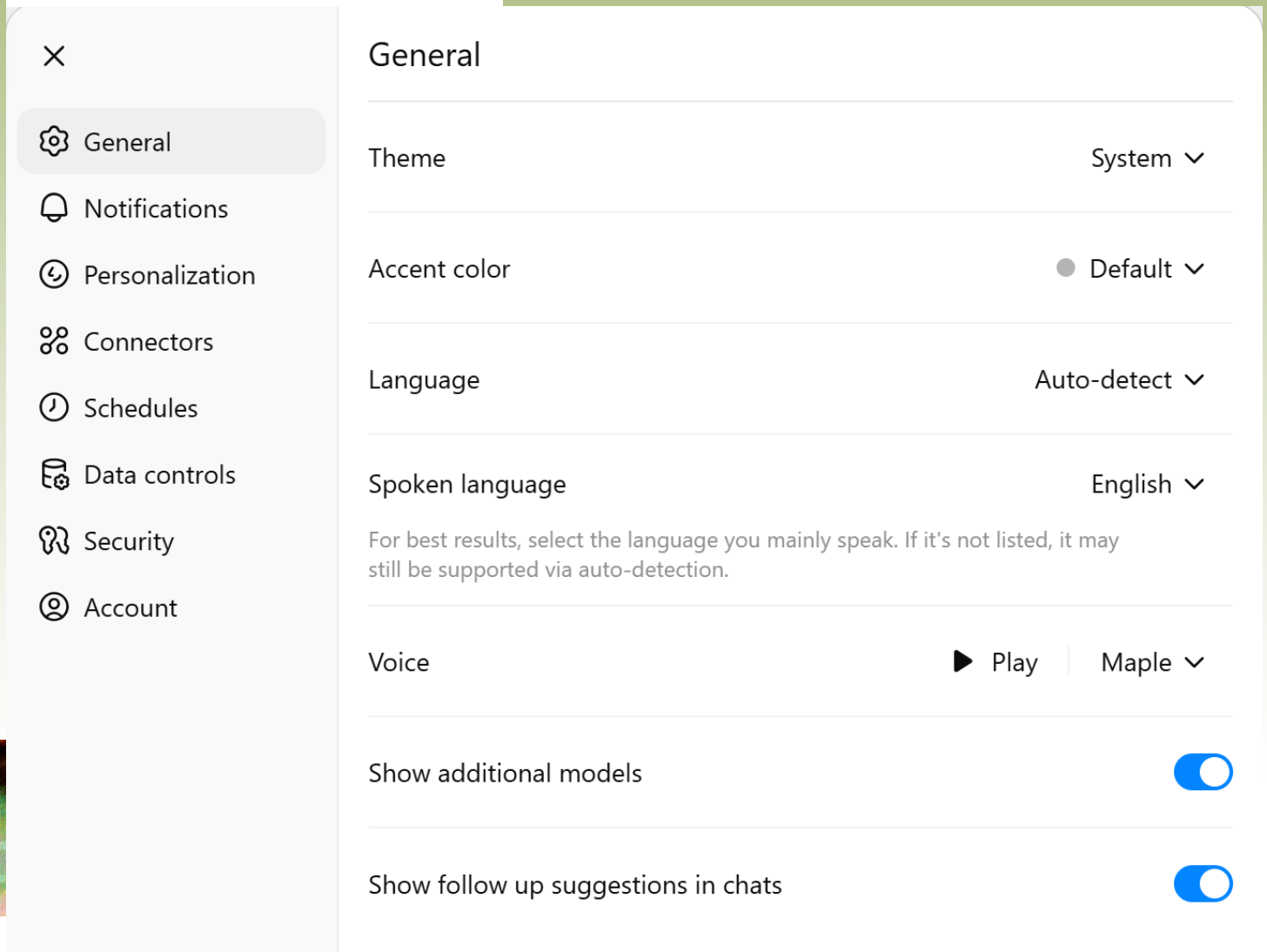
Opt Out of Sharing Training Data with Large Language Models

- ChatGPT
- Gemini
- Claude
- CoPilot

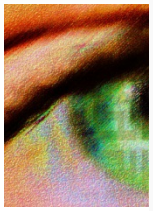
Eliminate Data Leakage!

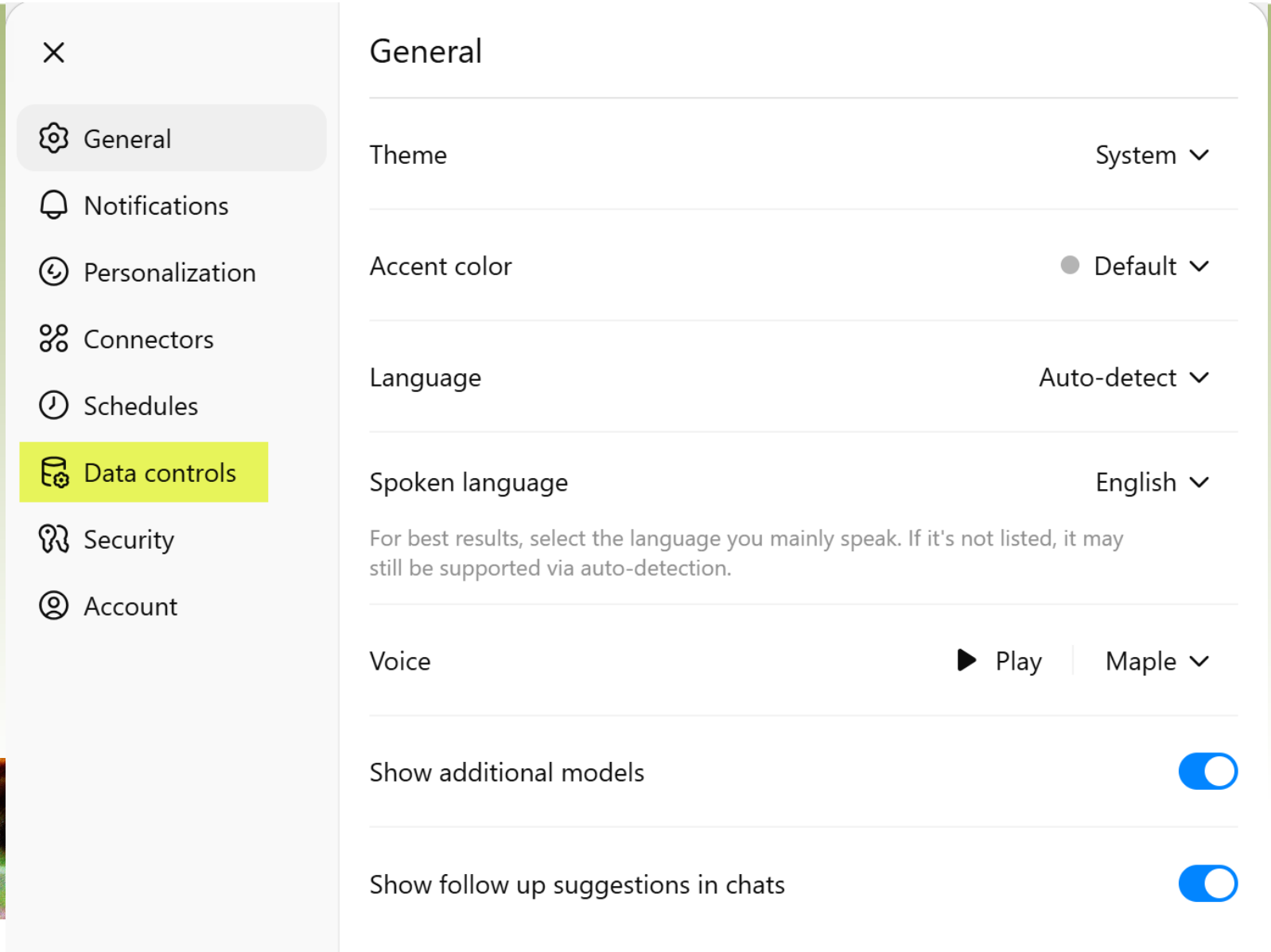
ChatGPT Plus Confidentiality

Settings

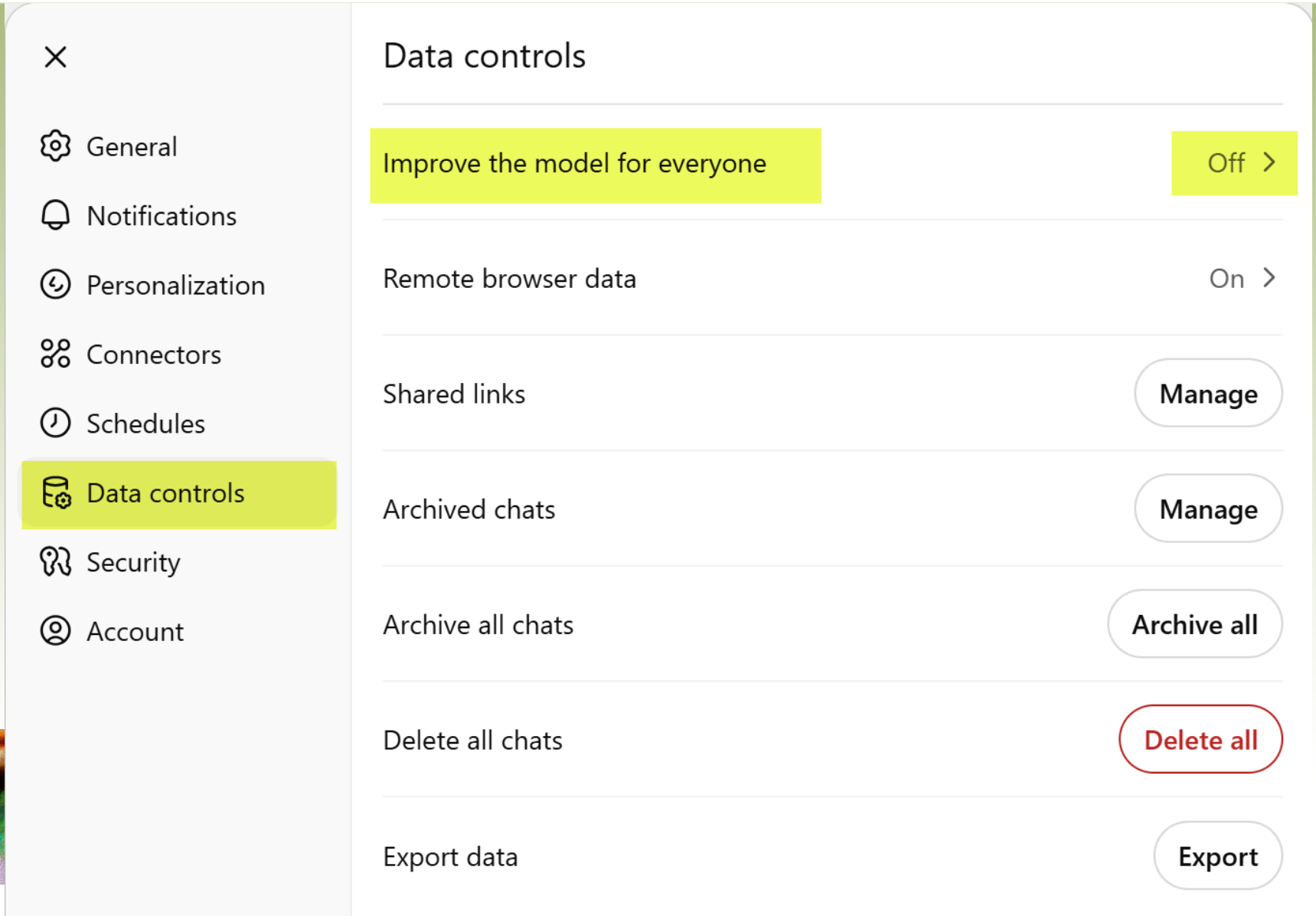


ChatGPT Plus Confidentiality

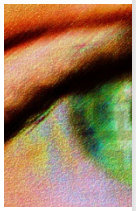




ChatGPT Plus Confidentiality



ChatGPT Plus Confidentiality



Data controls

General

Notifications

Personalizat

Connectors

Schedules

Data contro

Security

Account

Improve the model for everyone Off >

On >

Manage

Manage

Archive all

Delete all

Export

Model improvement

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

As Is

Voice mode

Include your audio recordings

Include your video recordings

Include your audio and video recordings from Voice Mode to train our models. Transcripts and other files are covered by "Improve the model for everyone." Learn more

Done

Gemini Confidentiality

Your Gemini Apps Activity

Gemini Apps give you direct access to Google AI. Your chats are saved in your account for up to 72 hours, whether Gemini Apps Activity is on or off. Google uses this data to provide the service, maintain its safety and security, and process any feedback you choose to provide.

Gemini Apps Activity
Saving activity

Turn off

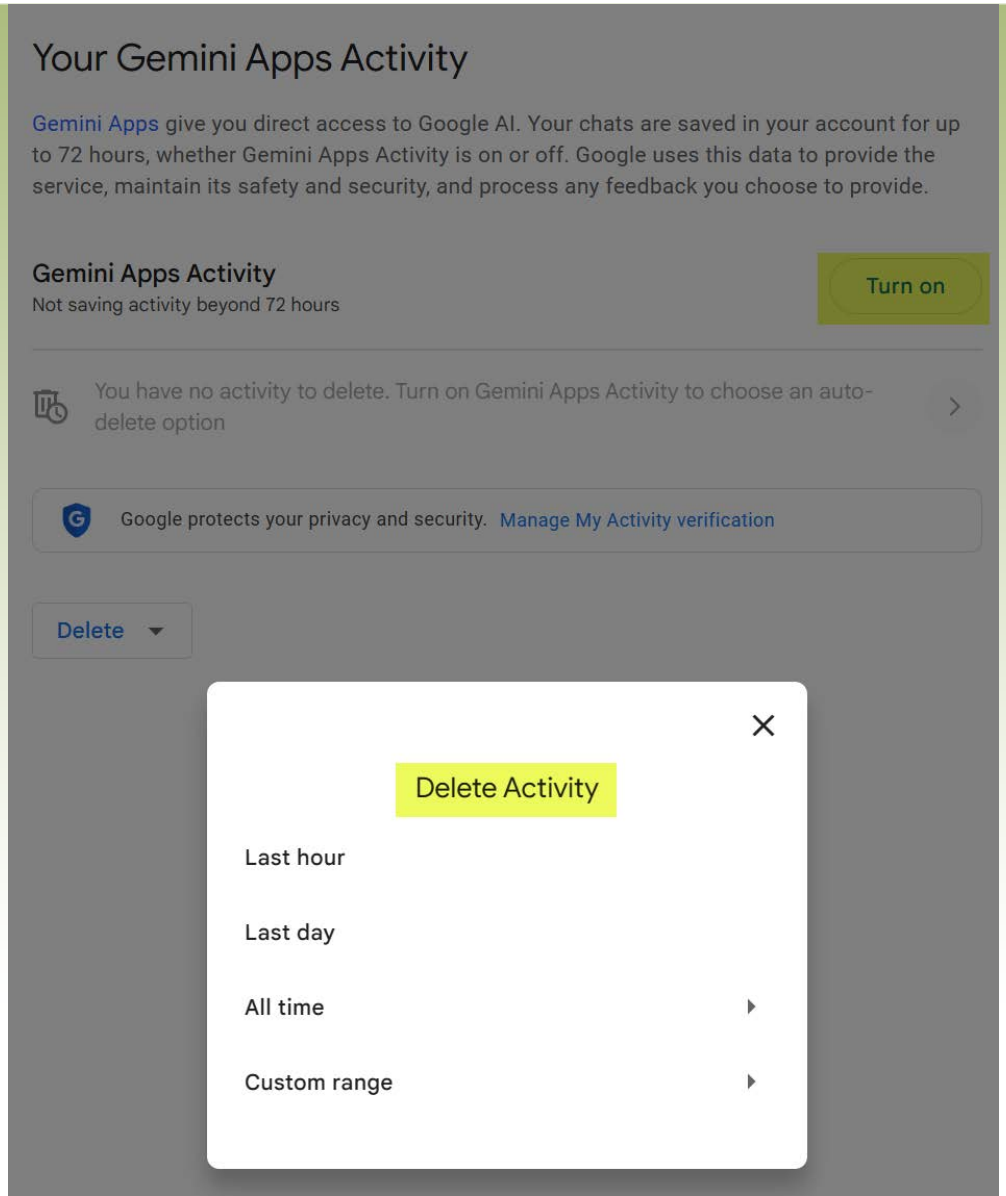
Turn "Activity" Off!

Deleting activity older than 18 months

Google protects your privacy and security. Manage My Activity verification

Delete

Gemini Confidentiality



Gemini Workspace 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 Workspace Confidentiality

Gemini app

Users

Groups

Organizational Units

Showing settings for users in **Test Org**

Gemini conversation history

Gemini conversation history
Applied at 'Test Org'

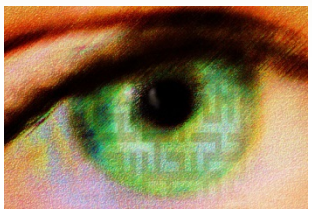
Gemini conversation history controls allow admins to control if conversations with Gemini are saved and for how long before they are automatically deleted. Disabling Gemini conversation history will not affect previous conversation history which is subject to the auto-delete setting below.

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



Claude Sonnet 4 – Free Plan

Settings

Profile

Account

Privacy

Billing

Features

Connectors

Claude Code

Full name

John Carney

What should Claude call you?

John

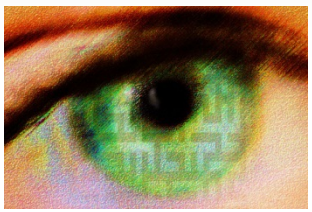
What best describes your work?

Select your work function

What personal preferences should Claude consider in responses? BETA

Your preferences will apply to all conversations, within Anthropic's guidelines. Learn about preferences

e.g. when learning new concepts, I find analogies particularly helpful



Claude Sonnet 4 – Free Plan

Settings

- Profile
- Account
- **Privacy**
- Billing
- Features
- Connectors
- Claude Code

Desktop app

- General
- Extensions
- Developer

Data privacy

Anthropic believes in transparent data practices

Keeping your data safe is a priority. Learn how your information is protected when using Anthropic products, and visit our Privacy Center and Privacy Policy for more details.

How we protect your data

- By default, Anthropic doesn't train our generative models on your conversations.
- Anthropic doesn't sell your data to third parties.
- Anthropic deletes your data promptly when requested, except for safety violations or conversations you've shared through feedback.

How we use your data

- Anthropic may use conversations flagged for safety violations to ensure safety of our systems for all users.
- Anthropic may use your email for account verification, billing, and Anthropic-led communications and marketing (e.g., emails sharing new product offerings and features).
- Anthropic may conduct aggregated, anonymized analysis of data to understand how people use Claude.
- Anthropic may offer additional features, which will enable us to collect and use more of your data. You'll always be in control and can turn off these features in your account settings.

Data controls

Export data — Export data

Shared chats — Manage

Location metadata

Allow Claude to use coarse location metadata (city/region) to improve product experiences. Learn more.

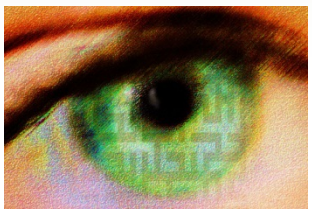
AI Confidentiality

Opt Out of Each Large Language Model

AI Tools that Use Multiple LLMs

(e.g. Perplexity)

Eliminate Data Leakage!



Perplexity Confidentiality

Account

- Account
- Preferences
- Personalization
- Tasks
- Notifications
- Connectors
- Pro Perks

Transactions

- Purchases
- Reservations

Account

jjc47639 — Change avatar

Full Name — Change full name

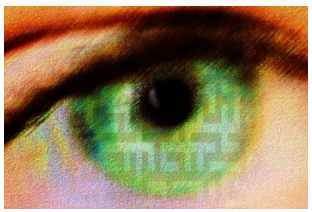
Username
jjc47639 — Change username

Email
jjc@carneyforensics.com

Subscription

Thanks for subscribing to Perplexity Pro!
Explore your new Pro features. Learn more

Manage plan ↗ | Upgrade plan



Perplexity Confidentiality

Preferences

Appearance
How Perplexity looks on your device
System (Light)

Language
The language used in the user interface
English

Preferred response language
The language used for AI responses
Automatic (detect inp...

Autosuggest
Enable dropdown and tab-complete suggestions while typing a query

Homepage widgets
Enable personalized widgets on the homepage

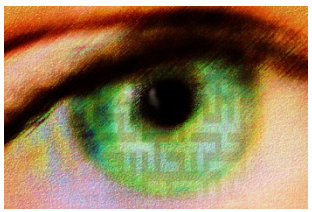
Artificial Intelligence

Model
Now includes Claude 4.0, GPT-4.1, and Sonar
Choose here

Image generation model
Default

AI data retention
AI Data Retention allows Perplexity to use your searches to improve AI models. Turn this setting off if you wish to exclude your data from this process.

Yes, default



AI Confidentiality

- Use Professional / Paid version of AI Tool
  - Not the Free Version
  - 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 Plus Security

Settings

- General
- Notifications
- Personalization
- Connectors
- Schedules
- Data controls
- Security
- Account

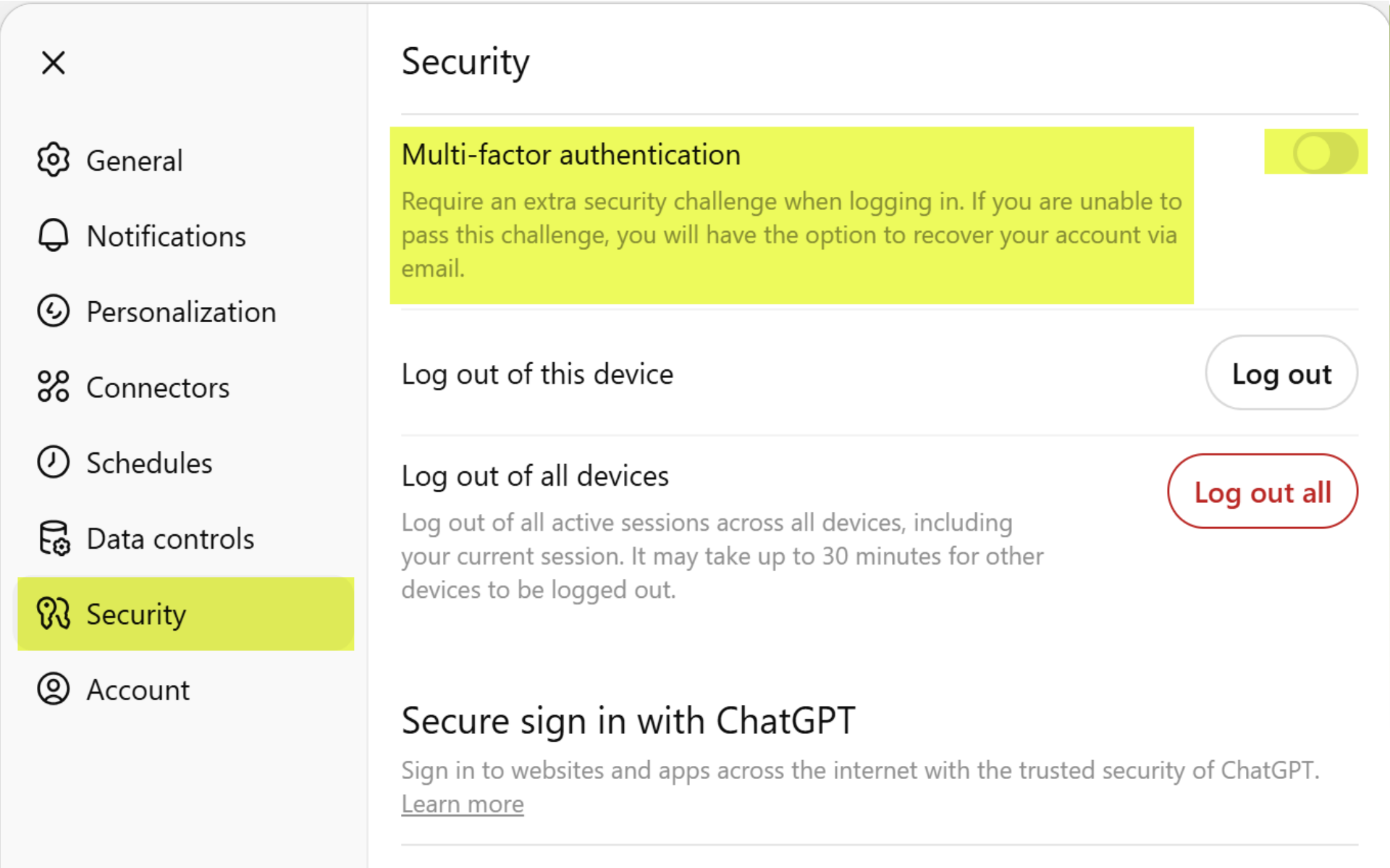
General

Theme	System
Accent color	Default
Language	Auto-detect
Spoken language	English

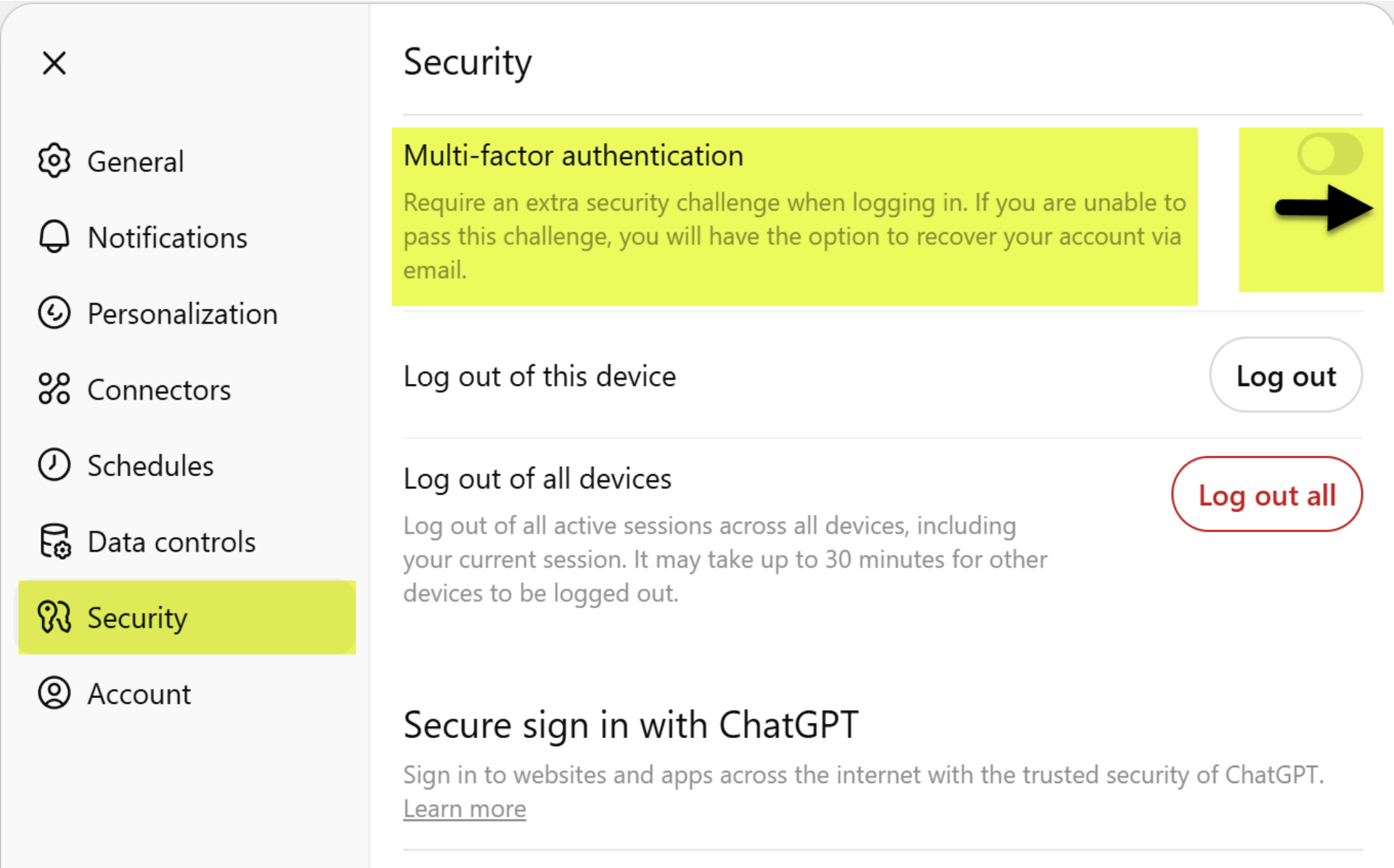
For best results, select the language you mainly speak. If it's not listed, it may still be supported via auto-detection.

Voice	Play Maple
Show additional models	
Show follow up suggestions in chats	

ChatGPT Plus Security

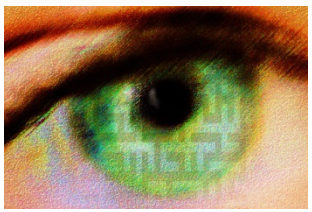


ChatGPT Plus Security



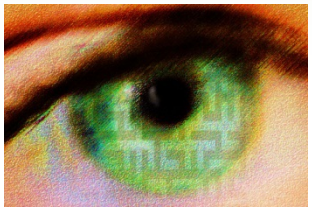
Two-Factor Authentication (2FA)

- 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

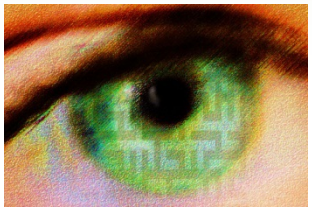
"For certain tasks, smaller models that are trained on more focused data sets can now perform just as well as larger ones—if not better. That's a boon for businesses eager to deploy AI in a handful of specific ways. You don't need the entire internet in your model if you're making the same kind of request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

Small Language Models (SLM)

SLM as an Alternative to LLMs

Legal Applications

- Law Firm Brief Bank
- MAJ, MDLA, MACDL Brief Banks
- All Your Firm's Practice Area Brief Bank
- All Your 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 Recognition / Categorization
  - 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

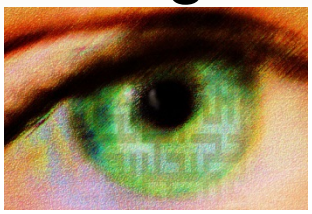
AI to Recover Digital Evidence

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

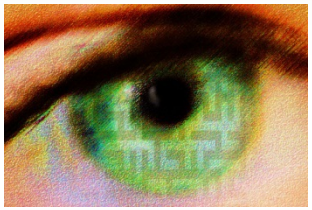
AI Vision and Auto-Identity and Search

- 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



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.

Future of AI Digital Forensics

AI Summarizes Messages, Emails, Documents, Notes, Searches

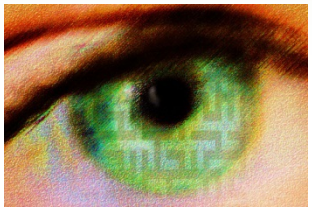
AI Automatically Generates Evidence Timelines for a Date Range

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

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

The Economist

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