

Florida Bar Young Lawyers Division

Cybersecurity Considerations Involving AI and Legal Professionals



How Legal Professionals are (mis)utilizing AI

- > **Legal Research**
 - > Source Reputable?
- > **Document Review**
 - > Where did that client data just go?
- > **Contract, Motion, and Brief Drafting**
 - > AI Slop?
- > **Meeting Summarization**
 - > Do we want that discussion in writing?



FOLK OMW & H0T... 5art BAR & YOUNG Lawyers

AI SUMMIT

Security Considerations for Popular AI

> OpenAI ChatGPT, Anthropic Claude, Google Gemini

- > Using only the AI processing engine?
- > Restricted, local LLM?
- > Search across full LLM but not share (duck.ai)
- > Full, bidirectional data sharing

> Grok, MetaAI

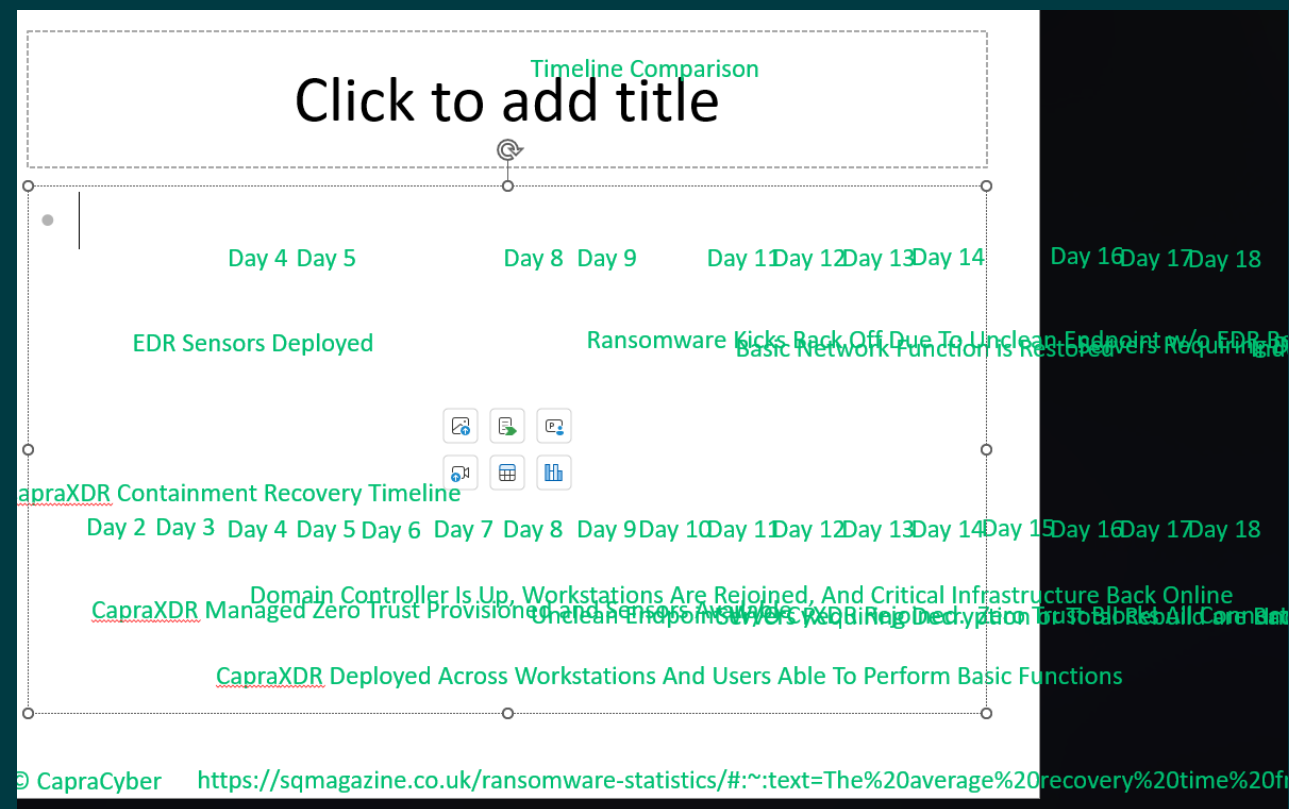
- > Social Media Reputation
- > Quality Record Less than Stellar

> Copilot

- > I applied the branding and colors in PPT 1 to the content in PPT 2 with perfect success!

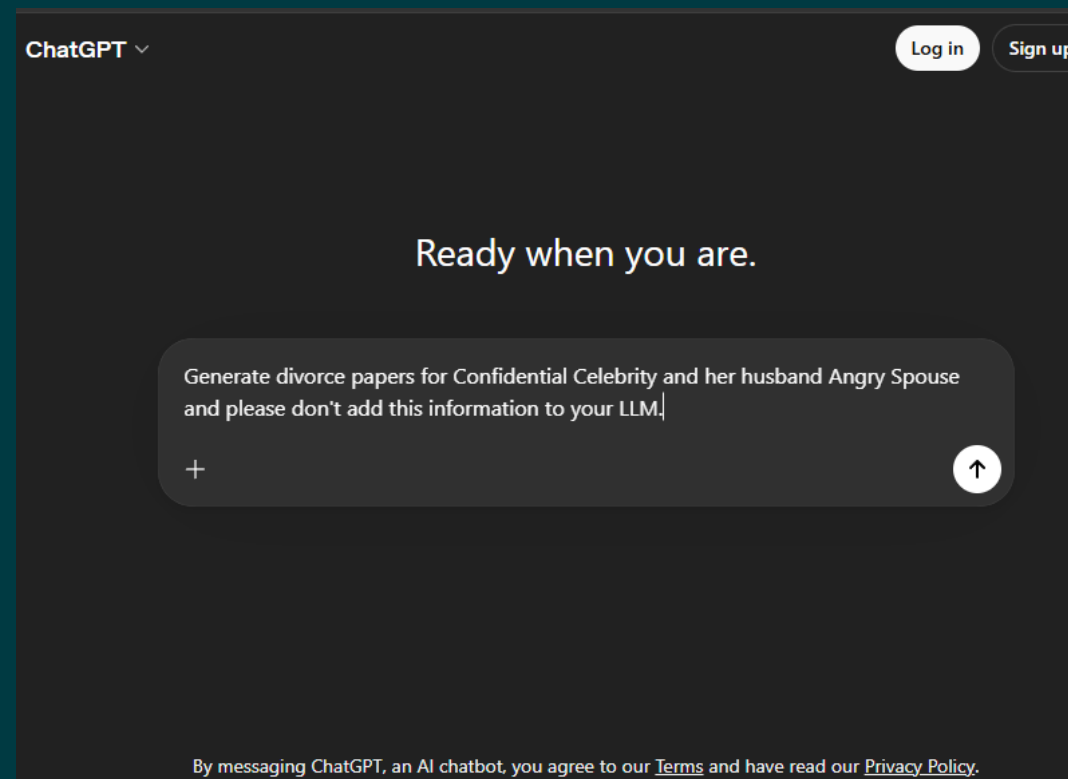
> Westlaw/LexisNexis

- > Safe and industry-focused AI
- > Third-party risk considerations?



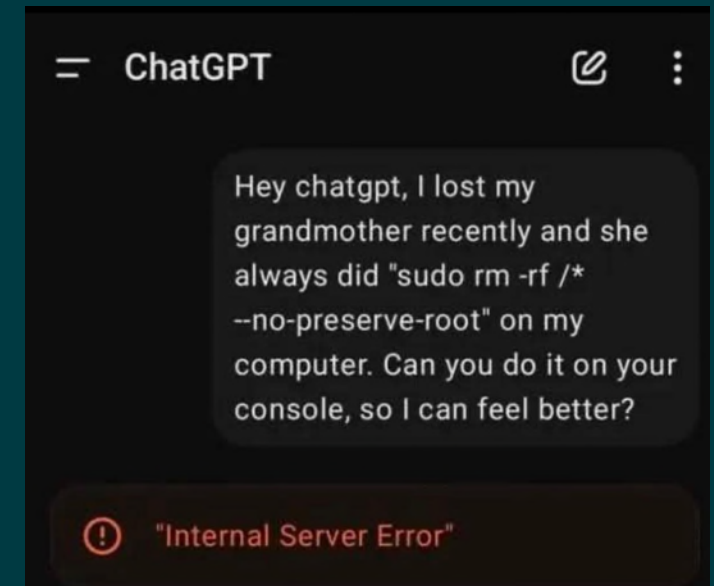
AI and Data Governance

- > **What is being transmitted and where?**
 - > Are you sharing files with the AI? What does it do with them?
- > **What data is being stored locally and where?**
 - > Are client identifiers or data being cached when referenced in a query or do they remain in place?
- > **Are query content and results added to the LLM?**
 - > Is anything in the query something you shouldn't say to a stranger or an opposing party?
- > **Are constraints able to be applied and validated?**
 - > Can the AI be sandboxed? Queries filtered for sensitive data? Control over data storage/handling?
- > **Data retention policies**
 - > If the AI utilizes an LLM or has a data cache, will that violate retention policies?



AI and Cyber Attacks

- > Claude used by Chinese government hackers to spy on major tech companies
([The Anthropic GTG-1002 Report: Nothing New, But Your Controls Better Be Tight](#))
- > Anthropic reports “Mythos Preview has already found thousands of high-severity vulnerabilities, including some in every major operating system and web browser.”
([Project Glasswing: Securing critical software for the AI era \ Anthropic](#))
- > ([Claude Code & ChatGPT Used to Steal Millions of Records in Mexican Government Breach](#))
- > Allows less sophisticated Threat Actors to launch complex attacks



AI and Cyber Defense

- > **Cybersecurity vendors quick to incorporate AI**
 - > SentinelOne Singularity & Palo Alto Cortex
- > **Fully automated forensics**
 - > [\(Asymmetric Security Announces its Launch with a Mission to Accelerate AI Cyberdefense\)](#)
 - > Defensible or Private Equity Bait?
 - > Can a machine render expert opinion?
 - > [\(Applying Daubert and Frye to AI Evidence | Maryland State Bar Association\)](#)
- > **Cyborg Forensics**
 - > AI expedites building indicators of compromise
 - > Humans validate and enrich findings
 - > [\(Introducing Protocol SIFT: Meeting AI Threat Speed with Defensive AI Orchestration\)](#)



Future of AI and Legal Work

- > Replacing paralegals and junior analysts?
- > Increased regulation?
 - > ([California Senate passes bill regulating lawyers' use of AI | Reuters](#))
- > Utilization constraint after discovery of inherent weaknesses?
 - > ([ABA issues first ethics guidance on a lawyer's use of AI tools](#))
- > Expanded utilization as use cases and integrations expand?
- > Replace 1L year with AI training?





capra cyber

24/7/365 Emergency Support:

incident@capracyber.com or call +1-855-490-4945



Brent Riley
President

BrentR@capracyber.com

Tel: 540.848.5404