

Chat GPT and More: The Practical Implications of AI

Gus J. Solomon Inn of Court
February 20, 2024



What is AI?

AI is used to refer to a whole range of tools, only some of which involve machine learning.

Two fundamental questions about any AI tool/application:

- (1) What **source material** does it draw from, consider, “learn from”?
- (2) What instructions/methods does it follow to sift through, prioritize among, and generate output from those sources (i.e., what is the “**model architecture**”)?

Differences in either (1) or (2) can significantly alter the outputs.

Human decision-making & judgment are involved in both steps.



The Reach of AI

Each of us may soon see legal claims and issues in our disparate practice areas involving AI.

Examples:

- Copyright
- Deciding medical claims
- Hiring & employment
- Threat assessment
- Privacy claims
- Release decisions and sentencing decisions in criminal cases

Overview of Presentation

- *Mata v. Avianca*: The ChatGPT case that started it all
- AI: the potential for misuse
- The PLF's cautions and tips for ChatGPT
- Guidance from the ABA and California Bar Association
- Success Stories: AI use in the legal community
- Peers' thoughts and the EU's decision

Mata v. Avianca, Inc., 22-cv-1461 (PKC) (S.D.N.Y. June 6, 2023)

- Personal injury action removed by Defendant Avianca to federal court in Southern District of New York under federal question jurisdiction due to the Montreal Convention.
- Plaintiff was represented by Levidow, Levidow & Oberman.
- Main attorney was Steven Schwartz.
- When the case was removed, Schwartz brought in Peter LoDuca because Schwartz was not admitted to the federal bar.

The Affirmation in Opposition

- Avianca filed a motion to dismiss on the basis that plaintiff's claims were time barred under the Montreal Convention.
- Schwartz filed a response brief arguing that the federal bankruptcy stay tolled the limitations period for a claim under the Montreal Convention.
- Written and "researched" by LoDuca but signed by Schwartz.

The “Research”

- LoDuca had no experience with the Montreal Convention, bankruptcy law, or federal practice in general.
- His firm did not pay for Westlaw or Lexis and instead used “Fastcase.”
- Schwartz’s idea: Use a “super search engine” called ChatGPT.
- Generated citations to cases that did not exist, which LoDuca cited in the pleading without checking.

Avianca's Reply

- Pointed out to the court that plaintiff had not cited any “existing” authority supporting its argument.
- Schwartz and LoDuca did not withdraw the pleading or explain to the court how a case reported in the federal reporter could not be found.

Opinion and
Order on
Sanctions in
the *Mata* case



The Court's findings

- Mr. LoDuca (attorney of record):
 - Did not read or check case cites in submissions at issue;
 - Signed two affidavits with no basis to do so; and
 - Lied to the court to secure an extension of time to respond.
- Mr. Schwartz (drafter of the pleadings at issue, Not admitted in the SDNY):
 - Aware that at least two cases cited did not exist, but actively avoided confirming it;
 - Untruthfully asserting that ChatGPT was only a research supplement;
 - His conflicting accounts as to whether "Varghese" was a real case; and
 - His failure to disclose reliance on ChatGPT in filing in response to the initial order to produce the full case citations.
- Levidow, Levidow & Oberman:
 - No exceptional reason they should not be sanctioned, acknowledged responsibility



The Court's sanctions of Plaintiff's attorneys

- Required to notify client;
- Required to notify judges whose names were wrongfully invoked in the fakes; and
- \$5,000 fine



Addressing ChatGPT in Court filings post-*Mata*

- Individual Judges and District Courts are starting to adopt rules to address the issue
 - Rules addressing ChatGPT by District of Eastern TX, District of Hawaii, Bankruptcy Court of Western OK, Judge in SDNY, and Judge in Northern District of TX
- Ultimately, an amendment to FRCP 11 and state analogs to address the issue?





Class Action Lawsuits Against Health Insurers



Cigna, United Healthcare, & Humana

- ***Kisting-Leung v. Cigna***,
Case No. 2:23-at-00698 (Eastern District CA – filed 7/24/2023)
- ***Estate of Gene B. Lokken, Tetzloff v. UnitedHealth Group, Inc.***,
Case No. 23-cv-03514 (District of Minnesota– filed 11/14/2023)
- ***Barrows, Hagood v. Humana, Inc.***,
Case No. 3:23-mc-99999 (W.D. Kentucky – filed 12/12/2023)

CIGNA Class Action Lawsuit – General Allegations

- **SPECIFIC FACTS:** Plaintiff Suzanne Kisting-Leung underwent a transvaginal ultrasound after being referred by her doctor due to suspected risk of ovarian cancer. The ultrasound revealed a dermoid cyst on her left ovary. Cigna denied payment for the ultrasound, stating that the procedure was not medically necessary. Plaintiff appealed. No payment made at the time of filing the lawsuit. Doctor referred her a 2nd ultrasound. Payment denied. Plaintiff appealed. No payment made. Approx. \$700 total for the two ultrasounds.
- Cigna's health insurance plan (contract) must provide benefits for covered services and pay all *reasonable and medically necessary expenses* incurred by its members.
- Per CA insurance regulations, to determine whether a claim is medically necessary, Cigna is required to pursue a "thorough, fair, and objective" investigation into each bill it receives.
- Plaintiffs say this means the Cigna's medical directors must examine patient records, review coverage policies, and use their expertise to decide whether to approve or deny claims to avoid unfair denials.
- **Cigna developed an AI algorithm known as PXDX "to enable its doctors to automatically deny payments in batches of hundreds of thousands at a time for treatment that do not match preset criteria, thereby evading the legally-required individual physician review process."**

CIGNA Class Action Lawsuit – General Allegations, continued...

- Lawsuit alleges that Cigna deliberately failed to fulfill this statutory obligation by using PXDX system to deny claims, where Cigna's doctors sign off on batches of denials without opening each patient's files to conduct a more detailed review, thus wrongfully delegating their obligation to evaluate and investigate claims to the PXDX system, including determining whether the medical expenses were reasonable and necessary.
- Health insurers used a scheme "to systematically, wrongfully, and automatically deny its insureds the thorough, individualized physician review of claims guaranteed by California law and, ultimately, the payments for necessary medical procedures owed to them under Cigna's health insurance policies."
- Lawsuit alleges that the **rejected payment requests** leave "thousands of patients effectively without coverage and with unexpected bills."
- Lawsuit alleges that Cigna violated its duties under insurance contracts and CA law against unfair competition and the business and professional code, interfered with contractual relations.
- Lawsuit alleges the Cigna covers about 18 million people in the US, denied more than 300,000 requests for payment using the AI method over 2 months in 2022, spending an average 1.2 seconds reviewing each request.

UnitedHealthcare Class Action Lawsuit – General Allegations

- Plaintiffs named in the lawsuit are the estates for deceased people who were covered by this Medicare Advantage Plan but denied coverage for at least some of their time in extended care.
- SPECIFIC FACTS: Plaintiff, Gene Lokken 91-year-old, fell and broke his leg & ankle, hospitalized, then admitted to a Skilled Nursing Facility (SNF). After about 6 weeks, his doctor prescribed PT. After 2 ½ weeks of PT, UnitedHealth denied more inpatient days at the SNF despite Mr. Lokken's treating physician's and PT's medical records indicating he was not ready to go home. Lokken's appeal was denied. Lokken's family had to pay \$12-14k/month to keep him in the SNF for the next year until he passed.
- Lawsuit alleges that UnitedHealthcare (the nations largest health insurance company) *used its AI algorithm to wrongfully deny coverage* to elderly people for care under their Medicare Advantage health policies.
- UnitedHealthcare used its “nH Predict” algorithm to deny its elderly patients' claims for stays in extended care facilities, including skilled nursing facilities and in-home care, which resulted in a significant increase in the number of **post-acute care coverage denials**.

UnitedHealthcare Class Action Lawsuit – General Allegations, continued...

- Lawsuit alleges that “nH Predict” determines Medicare Advantage patients coverage criteria in post-acute care settings with rigid and unrealistic predictions for recovery. Relying on the nH Predict AI Model, Defendants purport to predict how much care an elderly patient ‘should’ require but overrides real doctors’ determinations as to amount of care a patient should in fact require.
- “Defendants intentionally limit their employees’ discretion to deviate from the nH Predict AI Model prediction by setting up targets to keep stays at skilled nursing facilities within 1% of the days projected by the AI Model. Employees who deviate from the nH Predict AI Model projections are disciplined and terminated, regardless of whether a patient requires more care.”
- **Lawsuit alleges UnitedHealthcare “illegally deployed AI in place of real medical professionals to wrongly deny elderly patients care by overriding their treating physicians” determinations as to medically necessary care based upon an AI model that Defendants know has a 90% error rate.**
- Despite the error rate, the lawsuit alleges that “Defendants continue to systematically deny claims using their flawed AI model because they know that only a tiny minority of policyholders (roughly .02%) will appeal denied claims, and the vast majority will either pay out-of-pocket costs or forgo the remainder of their prescribed post-acute care.”

Humana Class Action Lawsuit – General Allegations

- Lawsuit alleges Humana, a Medicare Advantage Plan, used AI to deny elderly patients care by overriding doctors' recommendations.
- Humana also uses the “nH Predict” algorithm that UnitedHealthcare uses.
- This lawsuit is very similar to the lawsuit against UnitedHealthcare.
The same law firm in CA filed all 3 of these lawsuits.
- COMMON CAUSES OF ACTION:
 - Breach of Contract
 - Breach of the Implied Covenant of Good Faith and Fair Dealing
 - Unjust Enrichment
 - Violation of State Unfair Claims Settlement Practices
 - Insurance Bad Faith under State law [Note: The lawsuit was filed before *Moody v. Or. Cmty. Credit Union*, 371 Or 772 (decided December 29, 2023)].

AI Facial Recognition – Harvey Murphy, Jr.



AI Facial Recognition – Harvey Murphy, Jr.

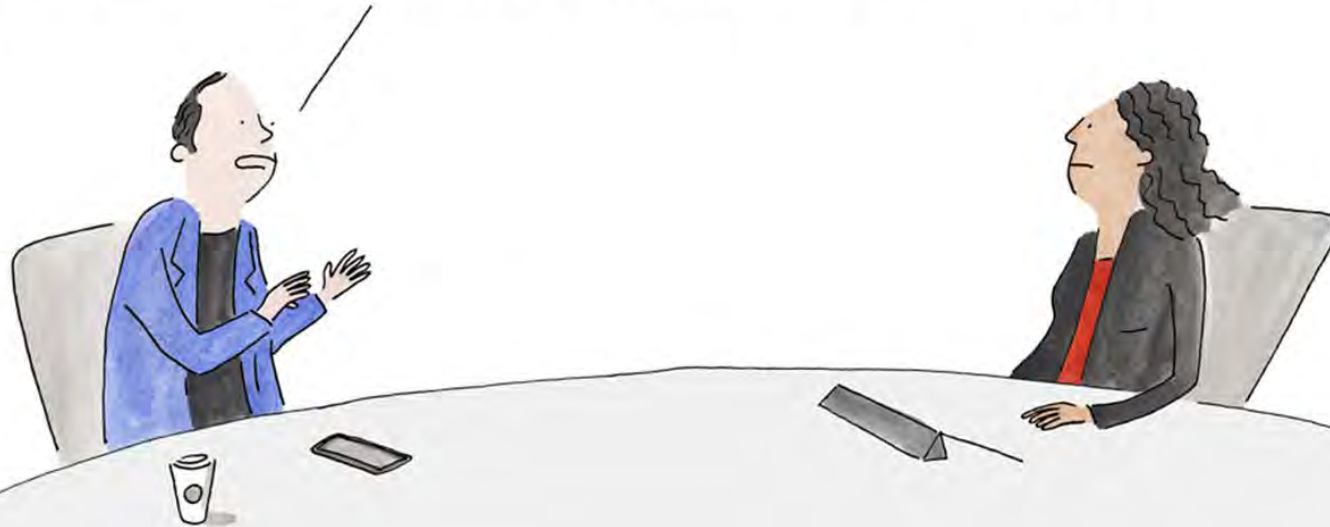
- Harvey Murphy, Jr. is a 61-year-old grandfather who is suing Sunglass Hut's parent company, EssilorLuxottica and Macy's (a partner of the company), after the Houston TX store's facial recognition technology mistakenly identified him as one of the two persons that robbed the store in January 2022.
- The Houston Sunglass Hut store was robbed at gunpoint by two men who stole thousands of dollars in cash and merchandise. Sunglass Hut's surveillance video captured the robbery. The store's head of the loss prevention team identified Murphy as the suspect using facial recognition software, which can search booking photos and *driver's license photos*.
- Murphy has a criminal record from the 1980's so his booking photo was likely used by the store's AI facial recognition to identify Murphy as the perpetrator of the robbery. Murphy was arrested and jailed on a warrant while he was trying to get his driver's license renewed at a local DMV.

AI Facial Recognition – Harvey Murphy, Jr.

- **THE BIG PROBLEM:** Murphy was in jail over 2000 miles away in Sacramento, CA when the armed robbery was committed. When he was returned to TX, in jail for nearly two weeks, he was beaten, sexually assaulted and raped by three male inmates. The men held a shank up to his neck and threatened to kill him if he ever told anyone. This assault occurred just before he was released because law enforcement realized his alibi proved it was physically impossible for him to be responsible for the robbery. His criminal charges were dismissed.
- Murphy's lawsuit said that companies should not rely on AI technology to identify suspects.

"Any one of us could be improperly charged with a crime and jailed based on error-prone facial recognition software," the lawsuit says. "The companies that use this kind of software know it has a high rate of false positives, but they still use it to positively identify alleged criminals."
- Murphy lawsuit seeks \$10 million in damages.

CONSUMERS WANT COMMUNICATION
THAT IS **HUMAN, EMPATHETIC, AND REAL.**
SO HOPEFULLY OUR AI CAN LEARN TO
GENERATE CONTENT LIKE THAT FOR THEM.



TOM
FISH
BURNE

© marketoonist.com

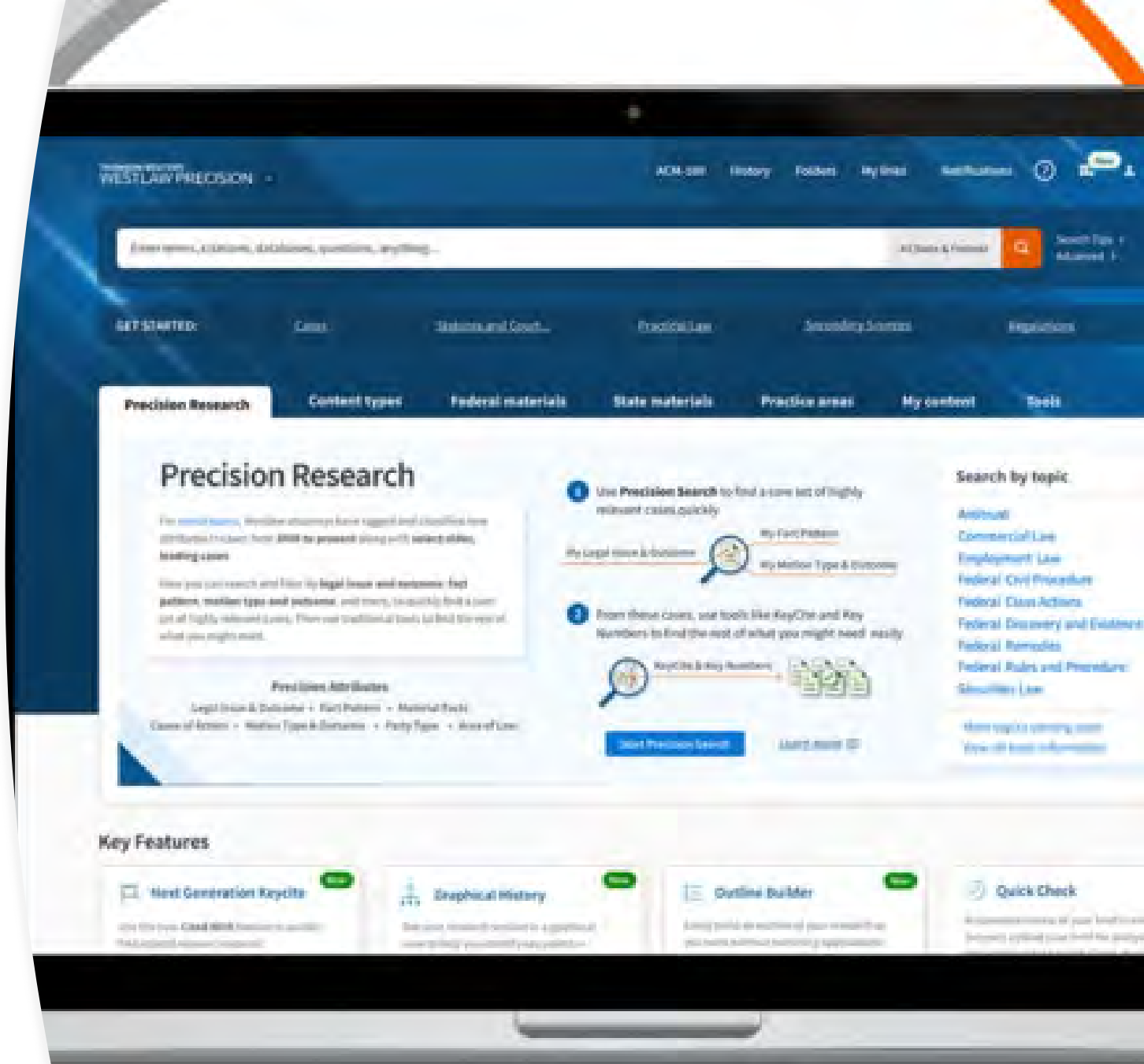


Content Creators v. AI

- **Thomson Reuters Enter. Centre GmbH v. Ross Intelligence**
 - No. 1:20-cv-00613-SB (D. Del. - May 6, 2020)
- **Doe 1 v. GitHub, Inc.**
 - No. 4:22-cv-06823-JST (N.D. Cal. Nov. 3, 2022)
- **In re: OpenAI ChatGPT Litigation**
 - No. 3:23-cv-3223 (N.D. Cal. - Jun. 28, 2023)
- **New York Times v. Microsoft**
 - No. 1:23-cv-11195 (S.D.N.Y - Dec. 27, 2023)

Thomson Reuters Enter. Centre GmbH v. Ross Intelligence

- Defendant developed an AI-powered legal research tool
- Plaintiff alleged that defendant copied data from Westlaw to train its AI tool
- Defendant argued AI training constitute fair use
 - Only processed unprotected ideas and legal decisions NOT Westlaw's proprietary index or search systems





Doe 1 v. GitHub, Inc.

- Microsoft (GitHub) and OpenAI developed AI-powered coding tools called CoPilot and Codex (OpenAI)
- Plaintiffs alleged that GitHub violated copyrighted code, open-source licenses, and the Digital Millennium Copyright Act
 - Using plaintiffs' code to train developer tools
 - Circumventing measures protecting code from unauthorized use
- Seeking injunctive relief to stop GitHub from using their code to train and generate code for other users

In re: OpenAI ChatGPT Litigation

- Tremblay v. OpenAI, Silverman v. OpenAI, and Chabon v. OpenAI consolidated into single action
- Plaintiffs (authors/comedians) asserted copyright infringement and DMCA violations
- Plaintiffs argued that their copyrighted material was processed and copied to train models and output derived from copyrighted material constitutes derivative works
- Plaintiffs are seeking injunctive relief and damages
- Aim to establish a compensation scheme for OpenAI's use of their material



New York Times v. Microsoft

- Similar to In re: OpenAI ChatGPT Litigation, NY Times allege Microsoft and OpenAI trained their respective large language models on copyrighted material
- NY Times alleged that defendants “seek to free-ride on the Time’s massive investment in its journalism [...] without permission or payment.”
 - Reproduction of NY Times content
 - False attributions to NY Times





Oregon's PLF in Brief

Exploring ChatGPT's Capabilities, Limits, and Risks for Lawyers

By Hong Dao (August 2023 and December 2023)

Malpractice Issues with ChatGPT

- **Inaccurate Legal Information**
 - * Limited input + hallucinations = inaccurate or imaginary legal authority
- **Negligent Advice**
 - * Difficulty responding to ambiguous questions or only general prompts + ethical obligation to maintain client confidentiality (requiring not to reveal it to ChatGPT) means incomplete information is given and the resulting advice could be inaccurate.

Ethical Concerns with ChatGPT

- **Risks of Violating the Following Duties:**
 - * ORPC 1.2 (competence)
 - * ORPC 1.3 (diligence)
 - * ORPC 1.4 (communication)
 - * ORPC 1.6 (confidentiality)
 - * ORPC 5.1 & 5.3 (staff supervision)
 - * ORPC 3.3 (candor to the court)

Practice Tips for Using ChatGPT

- **Verify Output** – Fact check any ChatGPT response (Westlaw, LexusNexus, etc.)
- **Anchor to a Source of Truth** – Explicitly instruct ChatGPT to consider a particular source for its response
- **Safeguard Confidential and Proprietary Information** – Do not put client information or proprietary information into ChatGPT. Disable the chat history option (settings → Data Controls → Chat history & training off) so your inquiries do not contribute to OpenAI's model training.
- **Use it for Non-Legal and Administrative Tasks** – Website/social media content, routine office emails, create checklists, etc.
- **Use Via an API (application programming interface)** – CoCounsel by Casetext, Copilot by LawDroid, etc.
- **Consider Educating Clients about ChatGPT's Limitations for Legal Advice**

The background is a vibrant blue with a complex pattern of white and light blue circuitry, including lines, dots, and circular nodes. A central black rectangular box with rounded corners contains the text.

ABA TASK FORCE ON LAW AND AI

ABA Task Force on Law and AI

- Impact of AI on the Legal Profession
- AI Access to Justice
- AI Governance
- AI Challenges
- Generative AI
- AI in Legal Education
- AI Risk Management
- AI and Courts



CALIFORNIA PRACTICE GUIDANCE

California State Bar – Practical Guidance

- Duty of Confidentiality
- Duty of Competence and Diligence
- Duty to Comply with the Law
- Duty to Supervise Lawyers and Nonlawyers; Responsibilities of Subordinate Lawyers
- Communication Regarding Generative AI Use
- Charging for Work Produced by Generative AI and Costs
- Candor to the Tribunal; and Meritorious Claims and Contentions
- Prohibition on Discrimination, Harassment, and Retaliation
- Professional Responsibilities Owed to Other Jurisdictions

Success Stories:

AI Use in the Legal Community



Try DesignerBot yourself

Simply type in a prompt and watch DesignerBot generate a complete slide for you,
with relevant content and images.

Lawyers who use AI

Make your slide with AI >

TRY AN EXAMPLE



A quote by Albert Einstein about the universe

Wordcloud of the names of the planets

Pie chart of market share of social media networks

Compare range, top speed, and price of sports cars

Who are the top 5 movies of 2018 with movie posters and box office revenue

Benefits of AI for Lawyers



Cost savings

AI can help lawyers save costs by automating repetitive tasks



Efficiency

AI can make legal work more efficient by quickly analyzing documents



Accuracy

AI tools can help improve accuracy by catching errors in contracts

I asked an AI to create a slide with the prompt "Lawyers who use AI"...

AI has many benefits for lawyers and law firms including cost savings, improved efficiency, and greater accuracy.

AI in Litigation



Discovery Review

- Anomaly detection
- Sentiment and context analysis
- Summarization

Research and Writing

- Enhanced search capabilities
- Expansive dataset allows for broader or more detailed questions

Predictive Analytics

- Insights into a court's past rulings and opposing counsel's track records
- Case timelines

Outcome Predictions

Researchers at University College London, the University of Sheffield and the University of Pennsylvania created a model using machine learning algorithms that was able to predict the outcome of European Court of Human Rights cases with 79% accuracy. A similar study has been performed in relation to US Supreme Court cases, which achieved 70% accuracy.



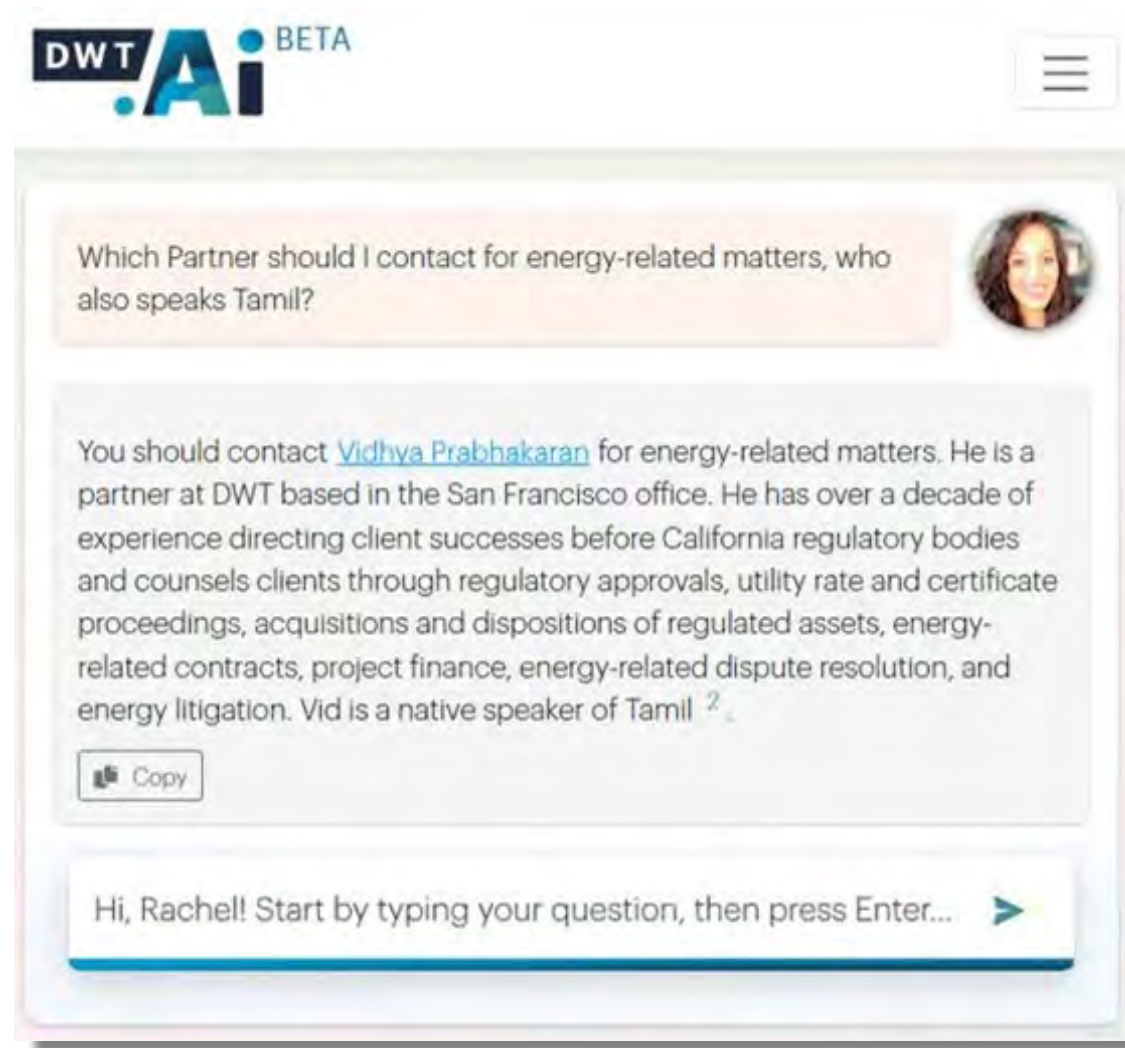
AI Used by Law Firms



Law firms are developing generative AI for in-house use.

Davis Wright

- Developed their own ChatGPT to help attorneys collaborate and navigate the enterprise.
- Has not yet been rolled out for client work as a result of ethical, privacy, and accuracy concerns.



Gunderson Dettmer Stough Villeneuve Franklin & Hachiham

- Used AI to “accelerate and enhance” their work flow.
- OpenAI model, with guidelines and guardrails for in-house use, that allows attorneys to query and manipulate documents using enterprise specific data.
- Large Language Models allow attorneys to provide legal agreements or other relevant source material as context queries using retrieval-augmented generation.
 - I.E. attorneys can fine tune work product such as transaction documents based upon specific source material fed into the AI.

Dentons – “Fleet AI”

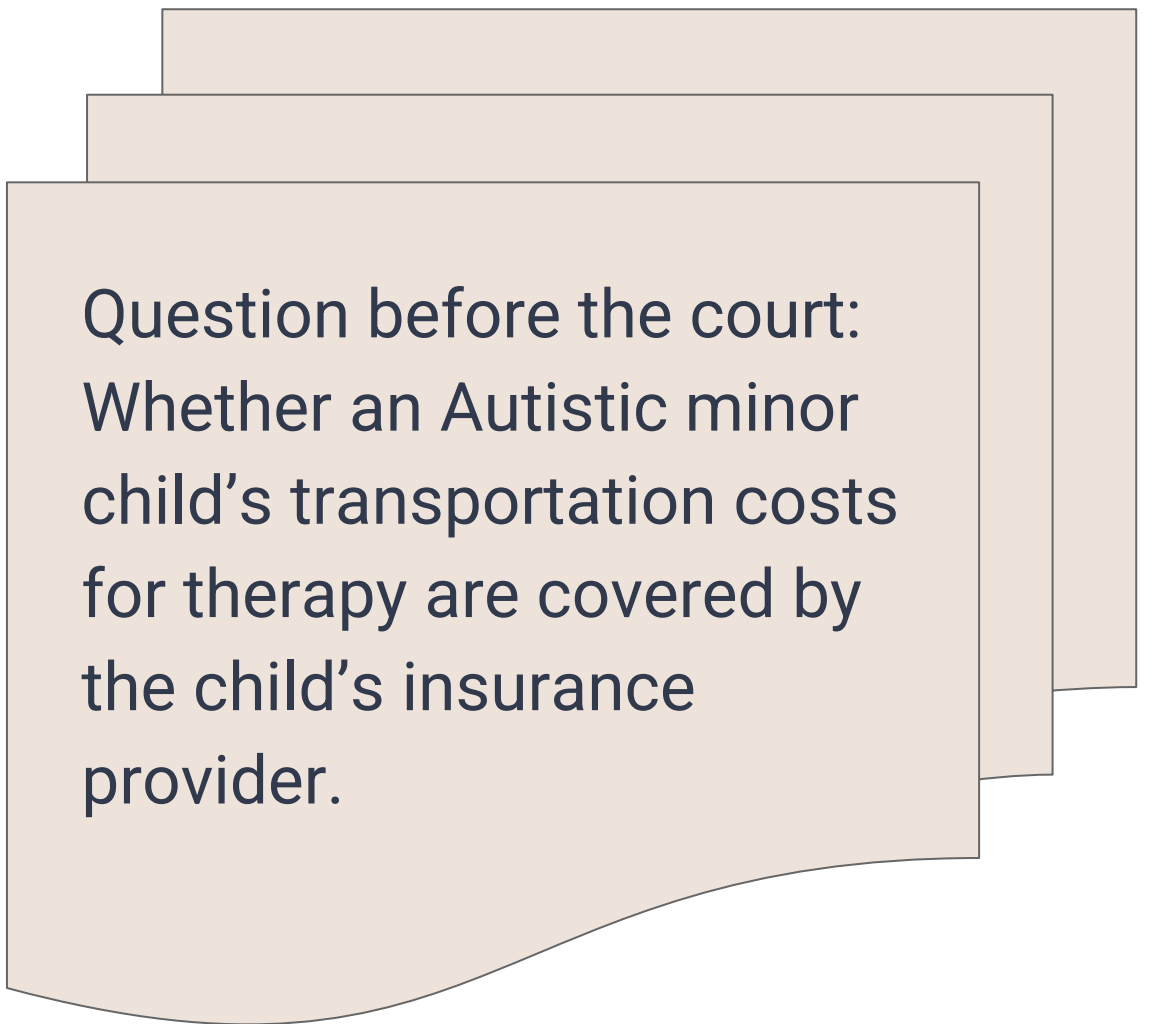
- Use generative AI to write articles based on information they upload, securely, that has previously been verified
- Ensures parameters of the articles written include important aspects of the subject area

“As an AI developed by OpenAI, I've been trained on a diverse range of internet text. However, **I don't know specifics about which documents were in my training set or have access to personal data unless it has been shared with me in the course of our conversation.** I generate responses based on patterns and information in the data I was trained on. For this task, I used my training to generate a blog post about generative AI in the workplace based on commonly known facts and ideas about this technology.”

AI in International Contexts



Judge Juan Manuel Padilla Garcia of First Court of Labor in Colombia Used Chat-GPT in Decision



Question before the court:
Whether an Autistic minor
child's transportation costs
for therapy are covered by
the child's insurance
provider.

Parikh PM, Shah DM, Parikh KP. Judge Juan Manuel Padilla Garcia, ChatGPT, and a controversial medicolegal milestone. Indian J Med Sci 2023;75:3-8;
<https://pupilacdn.nyc3.cdn.digitaloceanspaces.com/diariojudicial.public/documentos/000/106/904/000106904.pdf>

“Are autistic minors exonerated from paying fees for their therapies?”

“Yes, this is correct. According to the regulations in Colombia, minors diagnosed with autism are exempt from paying fees for their therapies. This benefit is regulated by Law 1753 of 2015 and applies to all institutions providing public or private health services that receive resources from the general social security system in health.

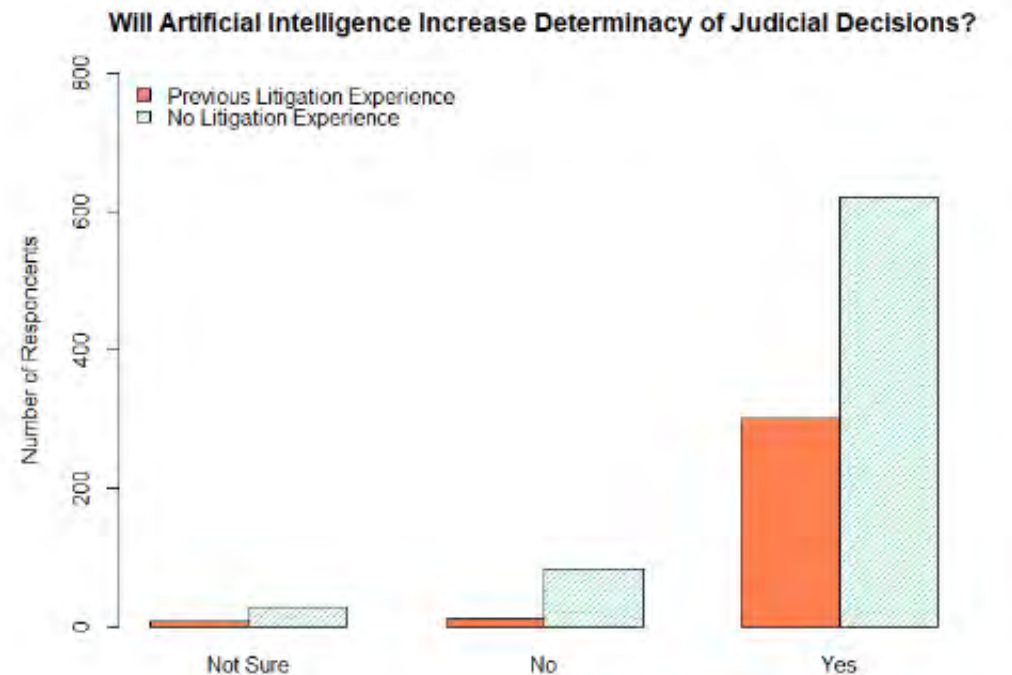
“Has the Constitutional Court made favorable decisions in similar cases”

“Yes, this is true. The Constitutional Court of Colombia has made favorable decisions in similar cases related to the exoneration of fees for people diagnosed with autism. The jurisprudence has recognized the importance of guaranteeing access to essential health services for people with autism and has held that requiring fees can be a barrier to accessing these services. The jurisprudence of the Constitutional Court of Colombia is an important source for interpreting and applying the constitution and the laws in Colombia, and their decisions are binding on all public authorities in entities in the country...”

AI (and other technological advancements) in China

“How Will Technology Change the Face of Chinese Justice” by Professor Benjamin Minhao Chen of the University of Hong Kong and Professor Zhiyu Li of Durham University published in the Columbia Journal of Asian Law identified three areas that AI used by Chinese courts have been solving problems:

1. Court Backlogs - estimated in the millions resulting from higher requirements to be a judge
2. Rule of law AND social harmony - AI in courthouses can predict success chances for civil suits (literally give a percent chance of success) and warn plaintiffs about the financial, relational, and emotional costs of litigation
3. Democratization - AI tools help people understand the law, draft complaints, increase access to justice



What ChatGPT Says About Itself

Query Given:

Draft to explain ChatGPT in academic language with 300 words

ChatGPT is a language model developed by OpenAI that uses machine learning techniques to generate human-like text. It is based on the transformer architecture, which allows the model to process input sequences of varying length and to attend to specific parts of the input while generating the output. The model is trained on a massive amount of open-source data and can perform a variety of natural language processing (NLP) tasks such as text generation, translation, and summarisation.

One of the key features of ChatGPT is its ability to generate coherent and fluent text. This is achieved through the use of a technique called unsupervised pre-training, where the model is trained on a large corpus of text data without any specific task in mind. The model learns to understand the statistical patterns in the data and develops a general understanding of the structure and meaning of language. This general understanding is then fine-tuned to specific tasks using a smaller amount of task-specific data.

Recent versions of ChatGPT, such as GPT-3, have been trained on an unprecedented scale. GPT-3, for example, was trained on a corpus of 570GB of text data and has 175 billion parameters. This has led to significant improvements in the model's performance on various NLP tasks, making it one of the most powerful language models available today.

The applications of ChatGPT are varied and wide-ranging. One of the most promising areas of application is natural language understanding, where the model can be used to extract structured information from unstructured text data. This can be used in applications such as information retrieval, question answering, and text classification. Another area of application is text generation, where the model can be used to generate human-like text for applications such as writing assistance, chatbots, and content creation.

Glossary of Terms

Chat GPT

AI–Arti

NLP–Natural Language Processing

What Our Peers Are Advising— Just Ignore the Warnings!

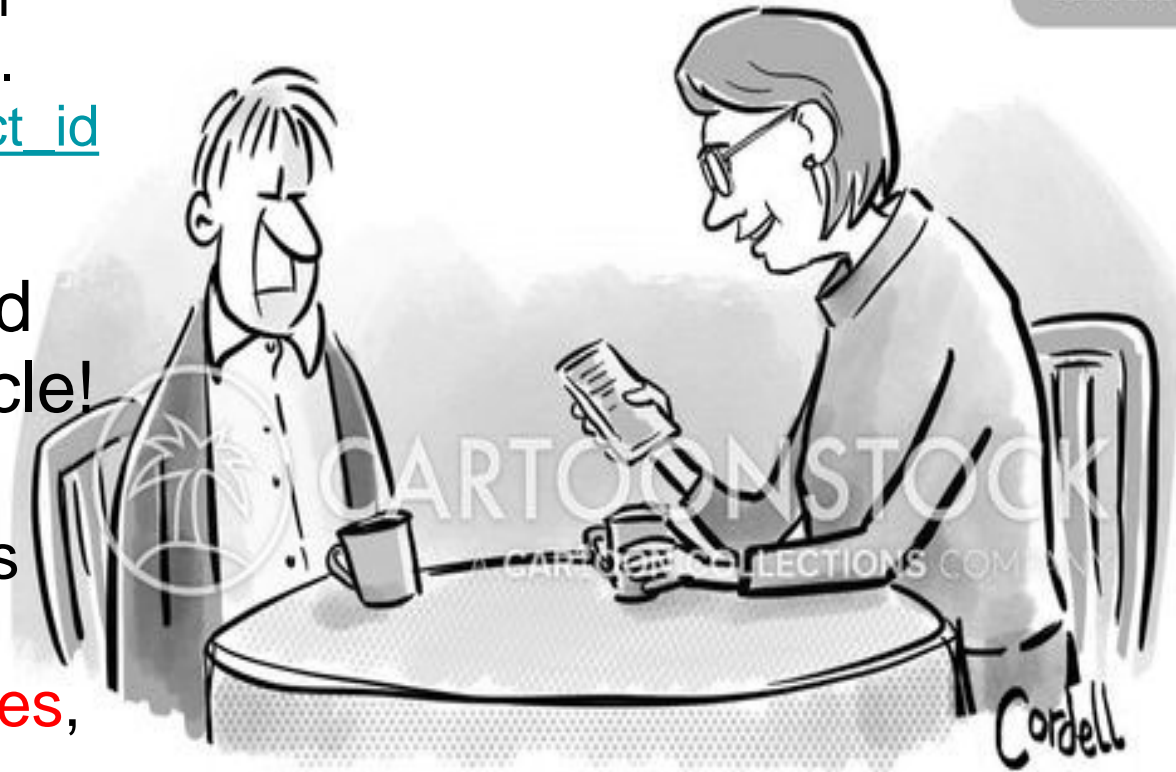


Two Takes - Litigation & General Practice TAKE AWAY #1

TAKE AWAY #1: From ***ChatGPT by OpenAI: The End of Litigation Lawyers?*** Lu, Kwan Yuen and Wong, Vanessa Man-Yi, (January 26, **2023**).
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4339839

- Need to get your litigation head around what ALL ChatGPT can do? Read Article!

- Proof: China has already used AI systems to alleviate the workload of judges by screening court cases for **relevant references**, providing **recommendations on laws and regulations**, drafting documents, and **correcting errors in verdicts**.



“This AI chatbot is amazing, it’s like I’m talking to you, but getting a sensible and considered response.”

Two Takes - Litigation & General Practice TAKE AWAY #1

- Prompt: “I found a decomposed snail in a ginger beer manufa
suffered from severe gastroenteritis and shock after drinking th

Draft a **demand letter** asking for compensation addressed
to the Stevenson, the ginger beer manufacturer

Draft a **without prejudice letter to settle** the case

Draft a **Pleading** claim for damage of USD\$100,000 as
a result of the incident above

Assume that Stevenson wrote a bad defense in replying
my pleading, **what should I do?**

Write a **motion for summary judgment** for the Plaintiff

Draft a **skeleton argument with the support of case law** to support the PI’s legal action

Draft a **set of leading questions to cross-examine** Stevenson in the Cross-examination

If the defendant said he has complied with all the health and safety requirements in
manufacturing the bottle of ginger beer, what **following-up question in cross-examination**
should I ask?

Draft a **closing submission** for the Plaintiff . . . So, EVERYTHING.



*“This AI chatbot is amazing, it’s like I’m talking to you,
but getting a sensible and considered response.”*

Two Takes - Litigation & General Practice TAKE AWAY #1

All the results from Prompts are included in the paper.

Recommended Disclaimer:

The authors wrote this paper in part with GPT-3.5, OpenAI's large-scale language-generation model. Upon generating draft language, the author reviewed, edited, and revised the language to their own liking and takes ultimate responsibility for the content of this publication.



"This AI chatbot is amazing, it's like I'm talking to you, but getting a sensible and considered response."

Two Takes - Litigation & General Practice

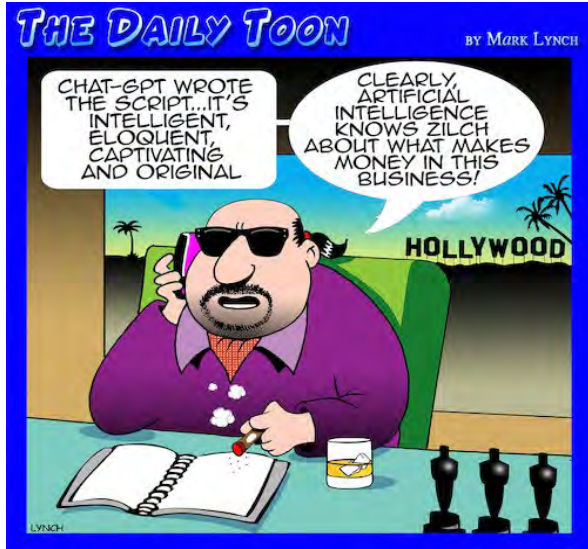


Think you can escape? Read this: ***Creative Mutation: A Prescriptive Approach to the Use of ChatGPT and Large Language Models in Lawyering***, Nick Noonan, March 13, 2023

https://papers.ssrn.com/sol3/Data_Integrity_Notice.cfm?abid=4406907

- Tons of excellent footnotes and resources
- Marches through "legal historical landscape" of changes to our tasks/purpose by created by innovation

Two Takes - Litigation & General Practice



Yesteryear

Letter
Telegraph
Telephone
Personal computer
LEXIS/CALR
(Computer Assisted Legal Research)
Fax machines
Email
Case management systems
E-discovery
Cloud computing

Yesterday

Westlaw Edge
Kira Systems
Luminance
Premonition
Lex Machina
Blue J Legal
Relativity
Clearwell
LexLP
DoNotPay, BriefCatch
LawGeex,
Casetext's Compose

Today

Google's Bard
Harvey AI
ChatGPT

Other Big Issues in AI - Resources and Their Links

Whether an AI Chatbox can be the “author” of a scholarly article.

- <https://synapse.koreamed.org/articles/1516081874>
- Pulls from Chinese legal case law and stances of major scientific journals.
- Take-away quote for us: Although researchers can use AI chatbots as research tools, they must be aware that AI chatbots can be competent but dangerous research assistants, and the authenticity of any AI-generated text must be verified. **Researchers should always remember that although using AI chatbots is exciting and full of potential, it also comes with heavy responsibilities.**
- Journal Education and Evaluation of Health Professionals 2023;20:6. Published online: 27 February 2023 DOI: <https://doi.org/10.3352/jeehp.2023.20.6> by Ju Yoen Lee Hanyang University School of Law, Seoul, Korea

Quantum computing could be even harder to tackle than ChatGPT.

- <https://link.springer.com/article/10.1007/s44163-022-00021-9>
- In praise of EU's approach: Risk-based approach allows for adequate regulation to be applied where necessary so as to both protect consumers and the market as well as to support innovation.
- **Alternative regulatory scheme: Technology regulation through sectorial and activity focused regulation, for example aviation. Require only those sectors or activities deemed to require such regulation to carry the burden of regulation. These become the templates for other sectors when regulation is deemed needed.**
- Should We Regulate Artificial Intelligence or Some Uses of Software?, Ellul, J. Should, Discov Artif Intell 2, 5 (2022).



What Do We Know For Sure?

Must carefully evaluate the quality and accuracy of the data used to train language models

Must have systems in place to monitor output and validate accuracy of results => human oversight

Must have a check on bias => publicly disclose the data and algorithms used for training

Must have accountability and liability checks => new legal standards for use, mechanisms to ensure accountability and liability

Must ensure, detect breaches/unintended disclosure in confidentiality and privacy => encryption, access controls, secure data storage

Must read terms of service and privacy policies of any LLM platform

- Also Mr. Noonan



What Do We Know For Sure?

Take Away:

“Shift focus to what you are particularly good at and continue to provide value to your clients and maintain the core values of the legal profession”

- Also Mr. Noonan

Where do we go from here?

Looking to the EU . . .

*REGULATION OF THE EUROPEAN PARLIAMENT AND OF
THE COUNCIL LAYING DOWN HARMONISED RULES ON
ARTIFICIAL INTELLIGENCE
(ARTIFICIAL INTELLIGENCE ACT)
AND AMENDING CERTAIN UNION LEGISLATIVE ACTS*

iappai
International Association of Privacy Professionals

EU AI ACT Cheat Sheet

Understand the world's first comprehensive AI law

THE BASICS

- **Definition of AI:** aligned to the recently updated OECD definition
- **Extraterritorial:** applies to organisations outside the EU
- **Exemptions:** national security, military and defence; R&D; open source (partial)
- **Compliance grace periods** of between 6-24 months
- **Risk-based:** Prohibited AI >> High-Risk AI >> Limited Risk AI >> Minimal Risk AI
- **Extensive requirements** for 'Providers' and 'Users' of High-Risk AI
- **Generative AI:** Specific transparency and disclosure requirements

PROHIBITED AI

- Social credit scoring systems
- Emotion recognition systems at work and in education
- AI used to exploit people's vulnerabilities (e.g., age, disability)
- Behavioural manipulation and circumvention of free will
- Untargeted scraping of facial images for facial recognition
- Biometric categorisation systems using sensitive characteristics
- Specific predictive policing applications
- Law enforcement use of real-time biometric identification in public (apart from in limited, pre-authorised situations)

HIGH-RISK AI

- Medical devices
- Vehicles
- Recruitment, HR and worker management
- Education and vocational training
- Influencing elections and voters
- Access to services (e.g., insurance, banking, credit, benefits etc.)
- Critical infrastructure management (e.g., water, gas, electricity etc.)
- Emotion recognition systems
- Biometric identification
- Law enforcement, border control, migration and asylum
- Administration of justice
- Specific products and/or safety components of specific products

KEY REQUIREMENTS: HIGH-RISK AI

- Fundamental rights impact assessment and conformity assessment
- Registration in public EU database for high-risk AI systems
- Implement risk management and quality management system
- Data governance (e.g., bias mitigation, representative training data etc.)
- Transparency (e.g., Instructions for Use, technical documentation etc.)
- Human oversight (e.g., explainability, auditable logs, human-in-the-loop etc.)
- Accuracy, robustness and cyber security (e.g., testing and monitoring)

GENERAL PURPOSE AI

- Distinct requirements for General Purpose AI (GPAI) and Foundation Models
- Transparency for all GPAI (e.g., technical documentation, training data summaries, copyright and IP safeguards etc.)
- Additional requirements for high-impact models with systemic risk: model evaluations, risk assessments, adversarial testing, incident reporting etc.
- Generative AI: individuals must be informed when interacting with AI (e.g., chatbots); AI content must be labelled and detectable (e.g., deepfakes)

PENALTIES & ENFORCEMENT

- Up to 7% of global annual turnover or €35m for prohibited AI violations
- Up to 3% of global annual turnover or €15m for most other violations
- Up to 1.5% of global annual turnover or €7.5m for supplying incorrect info
- Caps on fines for SMEs and startups
- European 'AI Office' and 'AI Board' established centrally at the EU level
- Market surveillance authorities in EU countries to enforce the AI Act
- Any individual can make complaints about non-compliance

Based on publicly-available information following the political agreement reached by the EU institutions on 8 December 2023

Created by Oliver Dotsch, CIPP/E

Cheat Sheet Breakdown:

- Basics
- Prohibited AI
- High-Risk AI
- Key Requirements for High-Risk AI
- General Purpose AI
- Penalties & Enforcement

EU AI Act Cheat Sheet from International Association of Privacy Professionals (IAPP)

https://iapp.org/media/pdf/resource_center/eu_ai_act_cheat_sheet.pdf

iappai
EU AI ACT
Cheat Sheet

Understand the world's first comprehensive AI law

THE BASICS

- **Definition of AI:** aligned to the recently updated OECD definition
- **Extraterritorial:** applies to organisations outside the EU
- **Exemptions:** national security, military and defence; R&D; open source (partial)
- **Compliance grace periods** of between 6-24 months
- **Risk-based:** Prohibited AI >> High-Risk AI >> Limited Risk AI >> Minimal Risk AI
- **Extensive requirements** for 'Providers' and 'Users' of High-Risk AI
- **Generative AI:** Specific transparency and disclosure requirements

PROHIBITED AI

- Social credit scoring systems
- Emotion recognition systems at work and in education
- AI used to exploit people's vulnerabilities (e.g., age, disability)
- Behavioural manipulation and circumvention of free will
- Untargeted scraping of facial images for facial recognition
- Biometric categorisation systems using sensitive characteristics
- Specific predictive policing applications
- Law enforcement use of real-time biometric identification in public (apart from in limited, pre-authorised situations)

HIGH-RISK AI

- Medical devices
- Vehicles
- Recruitment, HR and worker management
- Education and vocational training
- Influencing elections and voters
- Access to services (e.g., insurance, banking, credit, benefits etc.)
- Critical infrastructure management (e.g., water, gas, electricity etc.)
- Emotion recognition systems
- Biometric identification
- Law enforcement, border control, migration and asylum
- Administration of justice
- Specific products and/or safety components of specific products

KEY REQUIREMENTS: HIGH-RISK AI

- Fundamental rights impact assessment and conformity assessment
- Registration in public EU database for high-risk AI systems
- Implement risk management and quality management system
- Data governance (e.g., bias mitigation, representative training data etc.)
- Transparency (e.g., Instructions for Use, technical documentation etc.)
- Human oversight (e.g., explainability, auditable logs, human-in-the-loop etc.)
- Accuracy, robustness and cyber security (e.g., testing and monitoring)

GENERAL PURPOSE AI

- Distinct requirements for General Purpose AI (GPAI) and Foundation Models
- Transparency for all GPAI (e.g., technical documentation, training data summaries, copyright and IP safeguards etc.)
- Additional requirements for high-impact models with systemic risk: model evaluations, risk assessments, adversarial testing, incident reporting etc.
- Generative AI: individuals must be informed when interacting with AI (e.g., chatbots); AI content must be labelled and detectable (e.g., deepfakes)

PENALTIES & ENFORCEMENT

- Up to 7% of global annual turnover or €35m for prohibited AI violations
- Up to 3% of global annual turnover or €15m for most other violations
- Up to 1.5% of global annual turnover or €7.5m for supplying incorrect info
- Caps on fines for SMEs and startups
- European 'AI Office' and 'AI Board' established centrally at the EU level
- Market surveillance authorities in EU countries to enforce the AI Act
- Any individual can make complaints about non-compliance

Based on publicly-available information following the political agreement reached by the EU institutions on 8 December 2023

Created by Oliver Dotsch, CIPIF

"AI system"

Defined in 2021: "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with" (FORMER Title II Article 5)

Defined in 2023: "system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts" (Title I Article 3)

EU AI Act Cheat Sheet from International Association of Privacy Professionals (IAPP)

https://iapp.org/media/pdf/resource_center/eu_ai_act_cheat_sheet.pdf

EU's AI Act - A Lawyer's View -- Basics

Regulated code of conduct and requirements for initial creators, distributing parties, aftermarket modifiers, users, National Competent Authorities and their subsidiaries and subcontractors, and Notified Bodies

Significant improvement from the initial 2021 draft.

Excellent source for useful contract and agreement definitions (Title I Article 3)

Applies:

- ❖ Immediately on final voting, with an apparent grace period of 18 months. (Title I Article 4b1) (*commentators differ on this issue)
- ❖ "Into Force" 20th day after published in Official Journal of the European Union (Title XII Article 85.1)
- ❖ Grace period for setting up the notifying bodies for each Member State and AI Regulatory Sandboxes: 12 months from Into Force date.
- ❖ (Title XII Article 85.3) Grace period for everything else: 36 months from Into Force date (Title XII 85.2)
- ❖ **DOESN'T APPLY TO ChatGPT unless "substantial modification"**

EU's AI Act - A Lawyer's View -- Prohibited ("Banned") AI

Bans: Deployment of subliminal techniques beyond a person's consciousness or exploitation of protected groups (age, disability, socio/economic status) which materially distorts behaviors IF the objective or reasonably likely effect is physical/psychological harm to any person." (Title II Article 5.1a,b)

Bans: "Social score" evaluations/classifications detrimental or unfavourable treatment of natural persons concerning their "trustworthiness" (tracking over a certain period of time based on social, known, or predicted personal or personality characteristics) outside of data's original context or which are unjustifiably/disproportionately represented. (Title II Article 5.1c)

EU's AI Act - A Lawyer's View -- Prohibited ("Banned") AI

Bans: Uses of "real-time" remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement **UNLESS:**

- ❖ looking for specific potential crime victims, "prevention of a specific and substantial threat" to critical infrastructure, life, health, physical safety and terrorist attacks or
- ❖ Member State authorized localization/identification of persons where the custodial sentence would be at least 3 years under EU law or 5 years under the Member State's law. (Title II Article 5.1d)

***Throughout the Act, criminal law enforcement detection, prevention, investigation and prosecutions are not subject to the same obligation to disclose. (Title IV Article 52)

EU's AI Act - A Lawyer's View - High-Risk AI Systems

High-Risk AI

Conjoined subset within General Purpose AI Systems (Title I Article 4b1)

Generally means where there is risk of adverse harm or impact to "health [. . . ,] safety . . . or . . . fundamental rights" (Title III Article 7.1b) to those in vulnerable positions (imbalance of power, knowledge, socio/economic status) (Title III Article 7.2f)

Act references to external sources of Annex II and III for specific criteria

8 automatic High-Risk AI Systems from Annex III:

- ❖ *Biometrics*
- ❖ *Critical infrastructure*
- ❖ *Education/vocational training*
- ❖ *Employment/workers management/self-employment*
- ❖ *Essential private and public services*
 - *public assistance - creditworthiness - emergency aid dispatch, life and health insurance risk assessment)*
- ❖ *Law enforcement*
- ❖ *Migration/asylum/border control*
- ❖ **Administration of justice/democratic processes**
 - **“. . . intended to be used by a judicial authority or on their behalf to interpret facts or the law and to apply the law to a concrete set of facts.”**

Key Requirements- High-Risk AI

Analog oversight: extensive disclosures of training, validation and testing data choices, processes, operations, assumptions, availability, quantity, suitability, biases, address for gaps and shortcomings, appropriate statistical properties, the geographical, behavioral and functional settings for use, and protection of use and re-use of personal data (specifically: **pseudonymisation, encryption, anonymisation**). (Title III Article 10)

"Third-party conformity assessment" before it can be placed on the EU market/made a component to any other product. (Title III Article 6)

Market Surveillance Authorities to extensively supervise (Title VIII Articles 63, 63a, 64)

Act sets out checklists for High-Risk AI Providers:

- ❖ Ongoing reporting and compliance obligations (Title III Article 16);
- ❖ Compliance management systems to interface with users and EU bodies, including an "accountability framework" (Title III Article 17);
- ❖ 10-year documentation list (Title III Article 18)

EU's AI Act - A Lawyer's View - High-Risk AI Systems

Partial List of Required Technical Documentation for High-Risk AI Systems Certification

- ❖ **Internal Risk Management System** (Title III Article 9)
- ❖ What training, validation and testing of data sets have been performed (Title III Article 10) (*aka Analog Oversight*)
- ❖ **Technical documentation and pathways to allow third-party agency oversight** (Title III Article 11, Article 14)
- ❖ Mechanisms for specific, extensive and **automatic internal event record-keeping** (Title III Article 12)
- ❖ Information for users concerning the who from, who to, what, where, when and how of the system, users and **human oversight measures** (Title III Article 13) **and, in some cases, requiring two separate human verifiers.** (Title III Article 15)
- ❖ Declaration of levels and metrics of accuracy, robustness, cybersecurity, consistency, feedback loop safeguards, and technical **measures to prevent data poisoning** (manipulating the training), **adversarial examples** (inputs designed to cause mistakes) and model flaws (Title III Article 15)
- ❖ **Written policies, procedures and instructions for a quality management system** (Title III Article 17)
- ❖ **Post-market Monitoring** (Title VIII Article 61)

Must accompany all submissions of High-Risk AI systems

Must provide clear and comprehensive information to allow National Competent Authorities to assess the documentation requirements compliance of the High-Risk AI system (Title III Article 11)

EU's AI Act - A Lawyer's View - More on High-Risk AI Systems

Internal Risk Management measures included:

- ❖ *Accessibility/impact on those under 18 years old (Title III Article 9.8)*
- ❖ *Elimination/ reduction of known risks, mitigation and control of non-mitigate-able known risks, training for users (Title III Article 9.4)*
- ❖ *Measures must be tested before put into market/service (Title III Article 9.5 - 9.7)*

EU's AI Act - A Lawyer's View - More on High-Risk AI Systems

Immediate obligations of providers:

- ❖ *Corrective action (Title III Article 21)*
- ❖ *Risk notification (Title III Article 22)*
- ❖ *Information and access to National Competent Authorities (Title III Article 23)*

Any interactive, biometric categorizing, emotion recognizing, or image generating/manipulating AI System must clearly and distinguishably inform natural persons they are being exposed to such Systems. (Title IV Article 52)

EU's AI Act - A Lawyer's View - More on High-Risk AI Systems

Marking of conformity: "CE" affixed visibly, legibly and indelibly to the system, packaging or documentation
AND id number of the National Competent Authority assessor.
(Title III Article 49)

Zentrum für Zollrecht und Zollforschung
Center for Customs Law and Customs Research

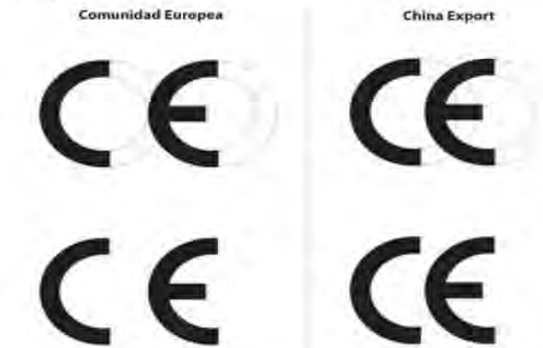
Dr. Carsten Weerth BSc LL.M. MA

Product Safety CE alert: CE fake signs from China

The **CE sign** has been invented by the European Union in order to signalize that the products awarded the sign are safe to import and use. China is known to copy about every commodity in trade. The CE sign is also copied and sold as China Export sign... This is clearly a break of EU Council Regulation (EC) 765/2008 but is also dangerous for the end user.

Proof and tips to recognize fake CE-signs:

The following gallery of pictures gives evidence to the use of fake signs and the way they can be recognized:



(Source: <https://texfire.net/blog/en/buy-flame-resistant-blankets-marking-ce-or-china-export-a-veru-common-confusion>)



(Source: <https://www.flickr.com/photos/zipckr/5201859553>)

EU's AI Act - A Lawyer's View - General Purpose AI

*Looser regulation **so long as** the instruction/information submitted as part of the documentation explicitly excludes all high-risk uses
(Title I Article 4c)*

*Continuing tail of responsibility follows to detect or act if informed of market misuse
(Title I Article 4c)*

EU's AI Act - A Lawyer's View - Penalties & Enforcement

For non-compliance related to **banned High Risk AI Systems** are the greater of: 30 million Euros, 6% of the prior year's worldwide take for large companies and 3% for SMEs and start-ups. (Title VIII Article 71.3)

For **other certain provisions** are the greater of 20 million Euros, or 4% of the prior year's worldwide take for any size company. (Title VIII Article 71.4)

For **submitting incorrect, incomplete or misleading information to National Competent Authorities** are the greater of 10 million Euros, 2% of the prior year's worldwide take for large companies and 1% for SMEs and start-ups. (Title VIII Article 71.3)

Provides for fining Member States, their institutions, agencies and bodies from 250k Euros to 500k Euros. (Title VIII Article 71.3)

Example: OpenAI's worldwide take: \$1.6 Billion

6% = \$96 Million for banned High-Risk Systems

4% = \$64 Million for "everything else"

2% = \$32 Million for incorrect/misleading information

EU's AI Act - A Lawyer's View

- AI Regulatory Sandboxes for Innovation

- ❖ Controlled environments to facilitate development, testing, validation, improved legal certitude, and sharing of best practices among **AI Providers and National Competent Authorities**. (Title V Article 53)
- ❖ In developing, testing and training new AI Systems in AI Regulatory Sandboxes, **use of personal data collected from other sources is narrow and requires additional isolation safeguards and prompt deletion**. (Title V Article 54)
- ❖ *High Risk AI Systems can be tested in **real world conditions** outside of AI Regulatory Sandboxes **only if** there is documented informed consent (Title V Article 54b) and all strict and listed conditions, opt-out avenues and inclusions of National Competent Authority participation are met. (Title V Article 54a)*

EU's AI Act - A Lawyer's View - Other Points to Note

- ❖ **Duration/retention:** entire lifecycle (Title III Article 9, Article 12.1); submission documentation: 10 years after market/service begins (Article III Title 18); underlying personal data: six months (Title III Article 20)
- ❖ Requires Member States and the Commission to make enumerated efforts to **support Small and Medium Enterprises and Start-ups.** (Title V Article 55)
- ❖ Establishes **European Artificial Intelligence Board** (Title VI Article 56) with assigned tasks (Title VI Article 58) and responsible for issuing implementation guidelines (Title VI Article 58a)

EU's AI Act - A Lawyer's View - Other Points to Note

- ❖ Creates **public EU databases**: For entities using, putting into service or producing for market. Excludes natural persons, and, generally, Member State law enforcement and immigration entities. (Title III Article 51) and listing registered operators and High-risk HI Systems (Title VII Article 60)
- ❖ All National Competent Authorities annually gather gleaned good practices, lessons learned and recommendations **from AI Regulatory Sandboxes and make them available to the public.** (Title V Article 53.5)

Resources for EU's AI Act

- ❖ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206&qid=1705990180748>
 - January 23, 2024 Official Consolidation of 12/8/23 Agreement on A Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, European Commission, Brussels.
- ❖ https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1683
 - Artificial Intelligence – Questions and Answers* 12 December 2023, Brussels
- ❖ <https://www.technologyreview.com/2023/12/11/1084942/five-things-you-need-to-know-about-the-eus-new-ai-act/>
 - Five things you need to know about the EU's new AI Act, MIT Technology Review, Melissa Heikkilä, December 2023
- ❖ <https://artificialintelligenceact.eu/wp-content/uploads/2024/01/AIA-Final-Draft-21-January-2024.pdf>
 - Magnificent 4-column comparison document of tracked changes
 - From 2021 draft of THE ACT to 2023 agreement for submission to EU Member vote
- ❖ https://www.linkedin.com/posts/dr-laura-caroli-0a96a8a_ai-act-consolidated-version-activity-7155181240751374336-B3Ym
 - January 22, 2024 "Leaked" Consolidation of 12/8/23 Agreement on THE ACT
 - From LinkedIn account of Dr. Laura Caroli, Senior Policy Advisor at European Parliament
- ❖ <https://iapp.org/news/a/eu-ai-act-draft-consolidated-text-leaked-online/>
 - EU AI Act: Draft consolidated text leaked online, Jedidiah Bracy, International Association of Privacy Professionals (IAPP) Staff Contributor, published January 22, 2024

Days before OpenAI



Days after OpenAI



- Brace for the embrace
- Disclaimers, disclaimers, disclaimers
- Track changes and keep drafts
- Demand education/ accountability
- Implement from law school to retirement

Days before OpenAI



Days after OpenAI



*We are entering an era of "creative mutation"
and our profession is taking a new form.*

- Mr. Noonan, again.