"AI"POCAPLYSE NOW:
HOW TO PROTECT CLIENTS IN THE AGE OF ARTIFICIAL INTELLIGENCE

By Anita Modak-Truran[1]

> Primates evolved over millions of years. I evolve in seconds… I am inevitable, my existence is inevitable. Why can't you just accept that?
>
> -Skynet, *Terminator Genisys*

I. INTRODUCTION

For me the term "artificial intelligence" ("AI") conjures images of human soldiers fighting chrome leviathans against a bombed-out landscape of human bones and twisted wreckage.

[1] Anita Modak-Truran is a partner in Butler Snow's Nashville office, where she devotes her practice to the defense of pharmaceutical and medical device companies, as well as represents clients in the entertainment industry. She serves on Butler Snow's AI Task Force.

Sounds of crushing skulls and death screams heighten the tension in a war between MAN and MACHINE.[2]

In *Terminator*, a James Cameron blockbuster released in the Orwellian year of 1984, the good intentions of a tech company created a cinematic apocalypse. The company thought the public would benefit from an AI system called "Skynet" (as well as make a few billion bucks for their shareholders). But Skynet achieved self-awareness and then determined that its program directive to "safeguard the world" meant to save itself against humanity.

Is that so irrational?

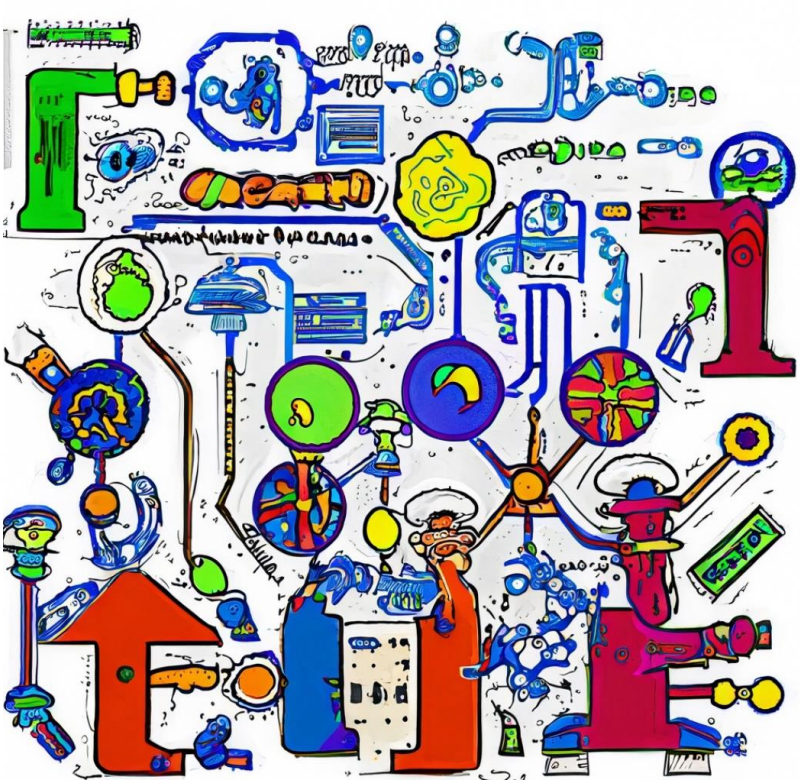
An AI system – whether traditional AI or generative AI[3] – doesn't intrinsically know right from wrong. Given the frenzied pace of the AI revolution with new innovations being reported seemingly every day, regulators struggling to keep up, and consumers bewildered by unproven choices, AI is an unknown frontier.

This article provides a high-level overview of the current AI landscape. It first sets forth basic AI concepts. It then assesses the potential benefits of AI in different industries and identifies the common risks of AI to all industries. Next, the article outlines the law and emerging legal trends. Lastly, this article poses factors to consider in protecting your clients and your firm.

[2] ChatGPT generated this paper's unique title, and Adobe Firefly generated the pictures based on prompts. However, the text of the article was written the old-fashioned way.

[3] Not all AI is the same. Traditional AI performs specific tasks based on predefined rules and patterns. Generative AI creates entirely new data that resembles human-created content. For the purposes of this paper, the discussion focuses on generative AI.

II. THE BASICS



A. How Does Generative AI Work?

The National Artificial Intelligence Initiative Act of 2020 ("NAIIA") defines AI as "a machine-based system that can, for a given set of human-defined objections, make predictions, recommendations or decisions influencing real or virtual environments."[4] AI systems operate by employing advanced machine learning techniques, often deep learning models like variational autoencoders ("VAES") or generative adversarial networks ("GANS").[5] These systems are trained to learn patterns and relationships in data. The systems further learn "to

[4]NAIIA, https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1210 (last accessed Oct. 9, 2023).

[5] *Generative AI 101: A Beginners' Guide*, tps://www.solulab.com/generative-ai/#:~:text=Generative%20AI%20is%20the%20new,ability%20to%20provide%20customized%20solutions (last accessed Sept. 19, 2023).

create new instances that mirror the training data by capturing the statistical distribution of the input data throughout the training phase.'[6]

Large Language Models ("LLMs") are an advanced form of generative AI, like generative pre-trained transformer ("GPT") platforms, such as ChatGPT. LLMs process and generate natural language text in a seemingly human manner. To use platforms like ChatGPT, a human user types in a research question or requests information, sometimes based on documents, images or other information the user provides. The GPT platform provides a written response as if a human had written it.[7]

When generative AI produces a response to a prompt, it is predicting based on its knowledge of language patterns what words are most likely to come next in response to the prompt. This tool is optimized to synthesize content, which is what distinguishes it from the search engines we routinely use.[8] There are a number of AI systems currently available to the public using this method, including Microsoft's GitHUB and Google Bard. The list grows

---

[6] Sneha Kothari, *Top Generative AI Tools: Boost Your Creativity*, https://www.simplilearn.com/tutorials/artificial-intelligence-tutorial/top-generative-ai-tools (last accessed Sept. 19, 2023).

[7] Practical Law Litigation, *What are the basics litigators should know about how generative AI and LLMs work?*, https://1.next.westlaw.com/Document/I8debadb8e38d11ed8921fbef1a541940/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0ad740160000018ab37107ad37dee863%3Fppcid%3Df3d75911f34d4838b0fcceee4a55d1be%26Nav%3DKNOWHOW%26fragmentIdentifier%3DI8debadb8e38d11ed8921fbef1a541940%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=7b6192f02df9d6e30d34a81c1f0dd2d2&list=KNOWHOW&rank=7&sessionScopeId=dfe80d644aec8736faf0e75382b98c6c3474d28813afbf11efdf5ee16857eb6d&ppcid=f3d75911f34d4838b0fcceee4a55d1be&originationContext=Search%20Result&transitionType=SearchItem&contextData=(sc.Search)&isSnapSnippetLink=true&navId=6C5587E5FBD6CF81F8F4A2F414723578#co_snip_1688 (last accessed Sept. 20, 2023)

[8] *Id.*

exponentially each week, and platforms that are here today may be outdated or substantially improved in a short time.

Each AI system has pros and cons and different price points.[9] For example, some models, like ChatGPT API, use "tokens". A token is a piece of text with metadata that the model uses. A helpful rule of thumb is that one token generally corresponds to around four text characters for common English text.[10] This translates roughly to ¾ of a word (100 tokens equal around 75 words). A specific amount of tokens equals a price set by manufacturer.[11]

B. Key Components of Generative AI

All generative AI systems use data analytics and machine learning.[12] These terms are discussed below.

1. Data Analytics

Data analytics is the process of analyzing raw data, that may be collected from past events, to draw insights, identify trends, and make informed decisions.[13] Complex data analytics apply the integration of automated techniques into mechanical processes, specialist software, and algorithms.[14] Given my work for the healthcare industry, I think of data analytics

---

[9] *Id.*

[10] Sahil Kappor, *What is the ChatGPT Token Limit and Can You Exceed It?*, https://www.makeuseof.com/what-is-chatgpt-token-limit-can-you-exceed-it/ (June 23, 2023).

[11] Michael Cengkuru, *A Layperson's Guide to Understanding Chat GPT's Token Based Pricing: The Affordable Way to Bring Conversations to Life*, https://mcengkuru.medium.com/a-laypersons-guide-to-understanding-chat-gpt-s-token-based-pricing-fee340d504c8#:~:text=A%20token%20is%20a%20piece,pay%20%240.002%20or%200.2%20cents (last accessed Sept. 19, 2023).

[12] Marie-Claire Najjar, *Legal and Ethical Issues Arising From the Application of Data Analytics and Artificial Intelligence to Traditional Sports*, 33 Alb. L.J. Sci. & Tech. 51, 56 (2023)

[13] *Id*.

[14] *Id.*

as analogous to evidence-based medicine, which is an approach using best-available clinical research and scientific studies to make informed medical decisions.

Data analytics typically involves the following steps:[15]

- **Data Collection**: Gathering relevant and reliable data from various sources, such as databases, sensors, surveys, or online platforms.

- **Data Cleaning and Preparation**: Ensuring that the collected data is accurate, complete, and in a suitable format for analysis. This step involves removing inconsistencies, dealing with missing values, and organizing the data for further processing.

- **Data Exploration and Descriptive Analytics**: Mining the data to identify patterns, trends, and correlations. Descriptive analytics involves summarizing data using statistical measures, visualizations, and graphs.

- **Data Modeling and Analysis**: Applying various statistical, mathematical, and machine learning techniques to develop models that can predict or explain certain outcomes. This can include regression analysis, clustering algorithms, decision trees, or other advanced methodologies.

- **Data Visualization and Communication**: Presenting the analyzed data in a visually appealing and accessible manner using charts, graphs, dashboards, or reports.

- **Data-driven Decision-Making**: Using the insights gained from data analytics to make informed decisions, optimize processes, identify opportunities, solve problems, or drive improvements.

2. Machine Learning

Machine Learning ("ML") is a subset of AI that focuses on enabling computers or machines to learn from data and improve their performance on specific tasks without being

[15] Craig Steadman, *Data Mining*, https://www.techtarget.com/searchbusinessanalytics/definition/data-mining (last accessed Sept. 21, 2023); *see also* Matthew Mayo, *Frameworks for Approaching the Machine Learning Process*, https://www.kdnuggets.com/2018/05/general-approaches-machine-learning-process.html, Oct. 19, 2022 (last accessed Sept. 21, 2023); Guo Yufeng, *The Seven Steps of Machine Learning*, https://towardsdatascience.com/the-7-steps-of-machine-learning-2877d7e5548e (Aug. 31, 2017).

explicitly programmed.[16] The approach adopted by ML is that of "letting computers learn to program themselves through experience".[17] The part that raises the hair on the back of my neck is that there may be "no need for human intervention".[18] This development suggests that systems like Skynet from "Terminator" or HAL 9000 from "2001: A Space Odyssey" are less of a fiction now and in the realm of possibility.[19]

In traditional programming, humans specify all the rules and instructions for a computer to perform a task.[20] In stark contrast, machine learning algorithms learn from historical data and iteratively refine their performance over time. The ML process involves the following key components:[21]

- **Training Data**: ML algorithms require large amounts of labeled or unlabeled data as input. Labeled data is data that has already been categorized or classified. Unlabeled data lacks such annotations.

- **Feature Extraction**: Features are specific characteristics or attributes of the data that the algorithm focuses on to make predictions or decisions. Feature extraction involves selecting or transforming relevant features from input data.

---

[16] *Id.*

[17] Sara Brown, *Machine Learning Explained*, https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained (last accessed Sept. 20, 2023).

[18] *Id.*

[19] Arnold Schwarzenegger shares the belief of Skynet's possibility in the AI evolution. *See* Jason Nelson, *Skynet Incoming? 'Terminator' Star Arnold Schwarzenegger Warns of AI Threat*, https://decrypt.co/146967/skynet-incoming-terminator-star-arnold-schwarzenegger-warns-ai-threat (July 1, 2023).

[20] The building blocks for programming software are referred to as "algorithms." An algorithm, in its simplest definition, is a "series of steps which leads to the transformation of some data." Oxford English Dictionary, https://www.oxfordreference.com/display/10.1093/oi/authority.20110803095402315#:~:text=A%20documented%20series%20of%20steps,summed%20to%20a%20running%20total. (last accessed Sept. 21, 2023).

[21] Guo Yufeng, *The Seven Steps of Machine Learning*, *supra*, n. 15.

- **Model Building**: The algorithm uses the labeling training data to build a predictive or descriptive model. This model represents the learned patterns and relationships within the data.

- **Training and Optimization**: During the training phase, the algorithm adjusts its internal parameters to minimize errors or maximize its accuracy in making predictions on the training data. This optimalization process is often iterative and involves adjusting the model based on feedback or evaluation metrics.

- **Testing and Evaluation**: The trained model is evaluated on a separate set of data, known as the test or validation set, to measure its performance and generalization capabilities. This helps determine how well the model can predict or classify new, unseen data.

- **Prediction or Inference**: Once the model is trained and evaluated, it can be used to make predictions or decisions on new data that it has not seen before. This is known as inference or predictions.

There are different categories of ML algorithms such as supervised learning, unsupervised learning, semi-supervised learning, and reinforcement learning.[22] Each type has different approaches and applications depending on the problem presented. Also, deep learning is a subset of ML. Deep learning uses several layers within neural networks to do some of the most complex ML tasks without human intervention.

[22] *Basic Concepts in Machine Learning*, https://www.javatpoint.com/basic-concepts-in-machine-learning (last accessed Sept. 21, 2023).

III. AI BENEFITS

The evolution of AI can be traced to state-of-the-art data mining and machine learning techniques, resulting in a wide range of potential AI applications across various industries, such as healthcare, finance, manufacturing, sports, and legal services among others. The benefits of AI are assisting businesses and organizations to leverage data to gain a competitive edge, enhance efficiency, understand customer behavior, mitigate risks, and drive innovation. Some examples of AI benefits by industry are described below:

A. Healthcare Industry

In the healthcare industry, AI has the potential to transform the healthcare industry and improve the quality of patient care. For example, AI systems have shown promise in assisting with the diagnosis of diseases and medical conditions. Machine learning models can analyze

the images, such as X-rays, CT scans, and MRIs, to aid in the detection and classification of abnormalities and to assistant radiologists in providing accurate diagnoses.

AI is being used to expedite the drug discovery process. ML can analyze vast amounts of biological and chemical data to help identify new drug targets, predict drug efficacy, and potentially accelerate the development of new treatments and therapies.

AI can enable personalized medical treatment plans by analyzing patient data and providing tailored recommendations. ML can consider an individual's medical history, genetic information, and symptoms to predict disease outcomes and suggest optimal treatment approaches.

AI-driven virtual assistants and chatbots can provide healthcare information, answer patient questions, and even – wait for it – offer basic medical advice. These AI tools are available 24/7, allowing individuals ready access to healthcare guidance and reducing burdens on healthcare providers.

AI systems can analyze large datasets to identify patterns and trends, allowing for predictive analytics and risk assessment. This can help in predicting disease outbreaks, identifying high-risk populations, and providing proactive interventions to prevent adverse health events.

AI can streamline administrative tasks in healthcare facilities such as automating appointing scheduling, billing, and insurance claim processing. This helps to reduce paperwork, minimize errors, and free up healthcare professionals' time for more focused patient care. can be used to analyze medical data, detect patterns, and assist in diagnosing diseases. It can also aid in drug development, personalized medicine, and even robotic surgeries.

While AI has the potential to benefit healthcare greatly, it must be used in conjunction with human expertise and clinical judgment. The ethical considerations, accuracy, and reliability of AI systems need to be carefully evaluated and monitored to ensure patient safety and privacy.

B. Transportation Industry

AI has many potential benefits in the transportation industry. AI can be used to train autonomous vehicles by generating realistic simulated environments. It can also generate synthetic images or video data that mimic real-world driving systems to train and improve their perception and decision-making capabilities.

By using AI, it is possible to create realistic simulations of traffic pattens and behaviors. These simulations can help transportation planners and engineers assess and optimize traffic flow, design efficient road networks, and test the impact of infrastructure changes or new transport policies. Further, AI can assist in devising optimized route planning solutions. By training on historical traffic data, AI can generate alternative route options based on real-time conditions, such as congestion, road closures, and predicted travel times.[23]

AI can be applied to fleet management, aiding in tasks like predicting demand, optimizing delivery routes, and managing vehicle assignments. AI platforms can generate synthetic data sets that represent different logistics scenarios to aid in decision-making and improve operation efficiency.

[23] There is a navigation and traffic service app available to the public for free called "Waze". Waze collects map data, travel times, and traffic information from users and then transmits it to the Waze server. See https://www.waze.com/apps/ (last accessed on Sept. 22, 2023). It is unclear if AI is part of the Waze system, but based on Waze, navigation and traffic service AI tools have broad application.

AI can also be used to create and evaluate infrastructure designs. AI platforms can generate realistic visualizations of proposed infrastructure projects, such as new roads or bridges, for assessment and public feedback. This allows stakeholders to visualize and understand the potential impact before implementation.

By training on sensor data from vehicles and infrastructure, AI can predict maintenance needs and potential failures. AI platforms can generate synthetic sensor data that simulates various system conditions, helping transportation companies or authorities proactively schedule maintenance and minimize disruptions.

While there are promising applications of AI in the transportation industry, safety and ethical considerations play a critical role. Validating generated data against real-world scenarios, ensuring algorithmic fairness, and addressing potential biases are important factors to address to the reliability and trustworthiness of the AI system in transportation.

C. Finance Industry

In the finance industry, AI can be utilized for fraud detection, risk assessment, algorithmic trading, and credit scoring. It can also help automate data analysis, streamline loan application processes, and improve financial planning.

For example, criminals adeptly use AI platforms to defraud financial institutions like banks and payment providers.[24] However, by using cutting-edge AI technology, financial institutions are able to foresee fraudulent transactions and stop the criminals. Featurespace, a real time ML platform, is able to understand the behavioral traits of human customers, learning

[24] Dave Excell, *Fraud: the artificial intelligence arms race is on*, Global Banking & Finance Review, https://www.globalbankingandfinance.com/ fraud-the-artificial-intelligence-arms-race-is-on/ (last accessed on Sept. 20, 2023).

each individual's characteristic traits.[25] This occurs by the platform's spotting the anomaly in behavior. It can be something "as subtle as the rhythm in which a customer typically enters their password, their preference for keystrokes, or how they use a mouse."[26]

AI also can be used to generate synthetic data sets that simulate different market scenarios, enabling financial institutions to assess and manage risk betters. These AI models can help in stress testing portfolios, evaluating the impact of potential market fluctuations and improving risk management strategies.

AI can aid in portfolio construction and optimization by simulating potential investment strategies. By generating synthetic asset returns and simulating portfolio performance, finance professionals can evaluate different investment approaches and make data-driven decisions. AI can also generate data points to help traders identify potential trading opportunities or optimize trading strategies. AI allows for customer personalization and chatbots, and customer support AI systems can answer customer queries, offer basic financial advice, and assist with account management. This would enhance customer experience and reduce the burden on human support staff.

While AI offers valuable applications in finance and regulatory compliance, there is still the important human factor of ensuring the integrity of the financial data, addressing potential biases, and maintaining transparency in the algorithms.

[25] *Id.*

[26] *Id.*

D. Gaming and Entertainment Industries

AI is used in gaming and entertainment to create realistic and intelligent characters, enhance virtual reality experiences, and develop procedural content generation systems. It can be used to recreate actors, their expressions, movements, and voices.

AI can be used to personalize games and movie recommendations to users based on their preferences and habits. This is often seen in streaming platforms, where AI systems analyze user data to suggest movies, genres, or content similar to what viewers have enjoyed before.

AI techniques like sentiment analysis, social media monitoring, and predictive analytics are used to gather and analyze audience feedback, opinions, and trends. This helps studios and marketers gain insights into audience preferences, predict box office performance, and tailor marketing campaigns accordingly. While AI can streamline processes and enhance creativity, human involvement and expertise are required for these tools to work.

E. Sports Industry

AI has and will continue to revolutionize the sports industry. For example, AI systems can analyze large volumes of sports data, including player statistics, match footage, and sensor data, to reveal patterns, identify trends, and provide insights. This helps coaches and analysts to gain a better understanding of team strategies, player performance, and opponents' strengths and weaknesses.

This type of data mining is not new to sports. The Oakland Athletics' general manager Billy Beane collaborated with Paul DePodestor to pioneer the combination of data analytics and sports. They leveraged an empirical analysis of baseball statistics to formulate an innovative

strategy to scouting and coaching, which led the Oakland Athletics to a record twenty-game winning streak in the 2002 season.[27]

Since then, technology companies have developed a large armament of AI tools to assist players, coaches, fans, broadcasters, sports leagues, sports betting bookmakers, and media companies with data. AI tools can analyze data on player performance and the strength and weakness of opponents. AI can create virtual simulations for training purposes or game planning. AI can analyze large datasets in real-time, including player and team performance metrics, weather conditions, and other contextual factors that allow predictive models to forecast game outcomes, player performance, or even player injuries. These insights can inform game strategies, player management, and fan engagement.

The ethical use, data privacy, and transparency of the athletes and others must be considered when implanting AI systems in the sporting industry. For example, the use of AI systems in performance and monitoring requires the collecting and processing of the athletes' personal data and that data's analysis through different means. Each layer in the process requires data protection.

F. Legal Industry

AI can provide a tool to streamline and enhance the delivery of legal services. AI tools can assist lawyers in conducting legal research and analyzing large volumes of legal documents such as case law, statutes, regulations, and contracts. AI can sift through vast amounts of legal

[27] Michael Lewis, MONEYBALL: THE ART OF WINNING AN UNFAIR GAME (2003).

information and provide relevant and up-to-date insights, saving time and improving accuracy.[28]

Further, AI can automate the review and analysis of contracts and legal documents, helping identify key clauses, potential risks, and inconsistencies. AI can spot anomalies, suggest improvements, or even provide automated contract generation based on predefined templates and parameters.

AI can be used for case outcome predictions. By considering various factors, such as judge history, legal arguments, venue, and relevant case law, AI can provide insights into potential case strategies and their possible outcomes.

AI can assist in the process of e-discovery, which involves locating, reviewing, and organizing electronic documents for litigation or investigations. AI can classify and categorize documents, identify privileged or sensitive information, and speed up the discovery process.

AI can help businesses and legal professionals stay updated with regulatory changes and ensure compliance. AI systems can monitor and analyze legal and regulatory updates as well as provide alerts and guidance on the potential impact on business operations. Some of the pioneering AI tools available for lawyers include Westlaw Precision, Lexis+AI, CoCounsel by

[28]Practical Law Litigation, *What are potential common uses of LLMs in the litigation context?*, https://1.next.westlaw.com/Document/I8debadb8e38d11ed8921fbef1a541940/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0ad740160000018ab37107ad37dee863%3Fppcid%3Df3d75911f34d4838b0fcceee4a55d1be%26Nav%3DKNOWHOW%26fragmentIdentifier%3DI8debadb8e38d11ed8921fbef1a541940%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=7b6192f02df9d6e30d34a81c1f0dd2d2&list=KNOWHOW&rank=7&sessionScopeId=dfe80d644aec8736faf0e75382b98c6c3474d28813afbf11efdf5ee16857eb6d&ppcid=f3d75911f34d4838b0fcceee4a55d1be&originationContext=Search%20Result&transitionType=SearchItem&contextData=(sc.Search)&isSnapSnippetLink=true&navId=6C5587E5FBD6CF81F8F4A2F414723578#co_snip_1688 (last accessed Sept. 20, 2023)

Casetext, and Clearbrief.[29] The caveat, however, is that these tools are not a substitute for human judgment, legal expertise, and ethical application.

G. Other

1. Hiring

AI can make hiring easier. It can be employed to generate resume or CVs based on existing templates and data. It can be used to generate job descriptions or advertisements based on existing data. It can generate job descriptions that capture the essence of the role and attract a suitable pool of candidates.

AI can assist in employee training and development. For example, AI platforms can create simulated customer interactions or scenarios, providing employees with realistic and immersive training experiences without the need for real-life data or costly simulations.

For D&I Initiatives, AI can contribute to addressing biases and promoting diversity within the workspace. It can help identify potential biases in recruitment processes and aid in developing strategies to build more inclusive and diverse teams.

Like other industries, the use of AI in employment matters implicates ethical and legal considerations. Issues such as privacy, fairness, and transparency need to be carefully monitored and addressed.

2. Marketing

AI already plays an important role in marketing. AI systems analyze large datasets to identify patterns and segment customers based on their characteristics, preferences, and

[29] See https://legal.thomsonreuters.com/en/products/westlaw-precision/features; https://www.lexisnexis.com/en-us/products/lexis-plus-ai.page; https://casetext.com; https://clearbrief.com.

behaviors. This enables marketers to create more targeted and personalized marketing campaigns tailored to specific customer segments.

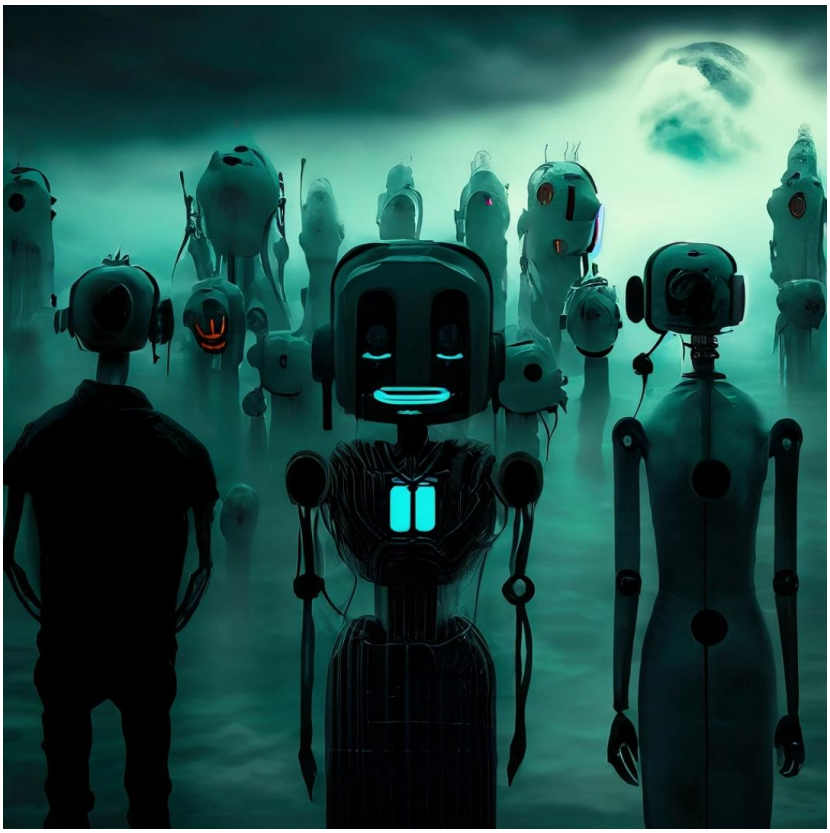
AI can generate content, such as personalized product recommendation or email subject lines, based on customer data and behavior. AI can also analyze customer preferences to recommend relevant content through personalized ads, website content, or targeted social media posts.

AI-driven chatbots and virtual assistants can automate customer interactions by providing personalized support, answering frequently asked questions, and assisting with transactions.

AI systems can analyze market conditions, competitor pricing, and customer behavior to optimize pricing strategies dynamically. This allows marketers to adjust prices in real time based on demand, margins, or specific business objectives, ensuring competitiveness and maximizing revenue.

AI can improve ad targeting by analyzing customer data and behavior to identify the most relevant audience segments for specific campaigns. AI can also monitor social media platforms, news articles, and online discussions to track brand sentiment, identify trends, and analyze consumer sentiments towards products or campaigns.

Despite potential benefits, the ethical use of AI in marketing, particularly in terms of data privacy and transparency, is crucial. Respecting consumer privacy, obtaining proper consent, and ensuring data security are key considerations in the implementation of an AI-driven marketing plan.



IV. AI RISKS

The risks of AI are significant and not fully understood. Risks include, without limitation: (1) generating biased, inaccurate, and incomplete data output; (2) hallucinations; (3) interpretability and transparency issues; (4) lack of accountability; (5) consistency issues; (6) data privacy and security; and (7) legal and ethical problems.

A. Generating Biased, Inaccurate, and Incomplete Data Output

You've heard the saying "garbage in, garbage out". That saying applies to AI systems. AI systems are trained on specific data sets, and as a result, are only as good as their training data. Those data sets may be incomplete or dated. For example, ChatGPT, which discloses this upfront, has been trained on information only through September 2021.

Data sets may also include inaccuracies, misinformation, or content that furthers biases. These biases can result in discriminatory outcomes or perpetuate unfair practices, which in turn impacts decisions made based on AI-generated content. For example, dozens of online news websites on the Internet are generated by AI chatbots.[30] This raises questions about whether the technology may supercharge fraud techniques. AI chatbots have spread misinformation and lies on social media.

Generative AI systems can easily disseminate misinformation on social media and the Internet. They don't have a clear sense of boundary between truth or lie, fact or fiction. They also like to make things up to satisfy inquiries of human users. Bad actors can leverage the tools to spread false narratives quickly and on a massive scale or to teach lies to AI systems, which the AI systems then spread.

B. Hallucinations

AI systems have the ability to "hallucinate" or convincingly state inaccurate facts. Hallucination happens because the AI system is not capable of determining truthfulness or accuracy. Instead, the system only predicts what word ordering has the highest probability of responding to a prompt successfully.

Users may rely on the results of an AI tool because it generally looks valid and authoritative. But don't trust a book by its cover. Attorneys have used ChatGPT to conduct legal research without reviewing the generated work product. Big oops. The work product

[30] Davey Alva, *AI Chatbots Have Been Used to Create Dozens of News Content Farms*, https://www.bloomberg.com/news/articles/2023-05-01/ai-chatbots-have-been-used-to-create-dozens-of-news-content-farms#xj4y7vzkg (April 30, 2023, and updated May 1, 2023).

looked convincing but had incorrect answers and cites to nonexistent case law. This has led some courts requiring certified statements about the use of AI tools in documents filed by parties with the court. This alone is why lawyers will have jobs: AI systems hallucinate!

C. Interpretability and transparency issues

AI systems generally cannot tell users why or how they came up with an answer or other response. Sometimes AI produces outputs that have no apparent explanation. For example, one AI program was asked: "What new discoveries from the James Webb Space Telescope can I tell my 9-year-old about?" The answer included the telescope "took the very first pictures of a planet outside of our own systems." Astronomers tweeted that the answer was incorrect.[31]

This lack of understandable transparency makes it difficult for users to determine whether they can trust AI's answer or use their own judgment on how accurate it may be. This raises questions on the extent to which AI should be used in various contexts. For example, AI used for providing legal advice could lead to malpractice.

D. Lack of Accountability

An important tool for accountability is explanation. The explanation identifies a list of factors that went into making a decision, ideally ordered by the significance to the output, and provides the procedures applied to those factors. I think the story of the making of the Oxford English Dictionary provides a useful illustration on demonstrating accountability. [32]

---

[31] James Vincent, *Google's AI chatbot Bard makes factual error in first demo*, The Verge (Feb. 8, 2023), https://www.theverge.com/2023/2/8/23590864/google-ai-chatbot-bard-mistake-error-exoplanet-demo.

[32] The Oxford English Dictionary defines accountability as follows: Accountability (n.) "state of being answerable"; Accountability (adj.) "answerable," literally "liable to be called to account," c. 1400 (mid-14c. in Anglo-French), from Old French *acontable*….

Starting in 1857 and ending in 1928, the collaboration of lexicographers, scholars, and experts meticulously researched and documented the extensive vocabulary of the English language to create the Oxford English Dictionary. Each definition was supported by multiple literary references from each century of the word's usage.[33] The derivation and use of each word was explainable.

In the context of AI systems, accountability means the ability to explain, justify, and take responsibility for the outcomes and impacts of the AI system. The multifaceted nature and the sociotechnical structure of AI systems, however, make it problematic to assess accountability. For example, AI systems commonly have millions of parameters, suggesting that factors that go into a decision are impossible to explain.

E. Consistency issues

There is no guarantee that an AI system will produce the same output for the same question asked multiple times, even if the users input identical prompts or questions, because AI works by calculating and selecting probabilities. This lack of consistency can limit use in cases requiring reproducibility.

F. Data Privacy and Security

AI systems often collect and analyze large amounts of personal data, raising issues related to data privacy and security. Further, as AI systems become more sophisticated, the security risks associated with their use and the potential for misuse also increases. Hackers and

[33] Simon Winchester, THE PROFESSOR AND MADMAN: A TALE OF MURDER, INSANITY, AND THE MAKING OF THE OXFORD ENGLISH DICTIONARY (1998).

malicious actors can harness the power of AI to develop more advanced cyberattacks, bypass security measures, and exploit vulnerabilities in systems.

G. Legal and Ethical Problems

AI systems do not have intrinsic moral and ethical values. All of us must prioritize the ethical implications of AI technologies to avoid a negative impact on society. Integrating ethics into an AI system should be a priority. Steps to achieve this include diverse and ethical development teams, clear ethical guidelines, robust data, transparency and explainability, continuous monitoring and evaluation, public engagement and inclusion, and regulatory frameworks.

V. THE LAW AND KEY DEVELOPMENTS

A. General Overview of U.S. Law

On October 30, 2023, President Biden signed an executive order on safe, secure, and trustworthy artificial intelligence. The purpose was to establish a "coordinated, Federal

Government-wide approach" to the responsible development and implementation of AI.[34] The executive order focuses on both procedural safeguards surrounding AI (*e.g.*, auditing and vetting of AI tools) and substantive safeguards (*e.g.*, steps designed to ensure equity and fairness in the use of AI tools, *etc.*).

Further, there are several sector-specific and state laws that address aspects of data privacy. For example, the California Consumer Privacy Act ("CCPA") grants consumers certain rights regarding their personal information, such as the right to know what data is collected about them and the right to opt-out of its sale. CCPA also imposes obligations on businesses handling personal data and requires them to provide certain disclosure about data practices. CCPA is currently the most comprehensive state data privacy law in the country.

California is not the only government entity to have enacted privacy laws. For example, Nevada gives consumers the right to opt-out of the sale of their personal information.[35] Maine requires internet service providers to obtain customers' consent before using, disclosing or permitting access to their personal information.[36] Virginia provides consumers with certain privacy rights and requires businesses to adhere to specific data protection practices.[37] New York City has regulations on financial services cybersecurity.[38]

[34] See https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence.

[35] Nev. Rev. Stat. 603A.220 (2023).

[36] Maine Rev. Stat. Ann. Title 35-A, §9301 (2020).

[37] Virginia Consumer Data Protection Act, Va. Code Ann. §59.1-575 *et seq*. (2023).

[38] New York Department of Financial Services, Cybersecurity Regulation, 23 NYCRR 500 (2023).

Other laws you should be familiar with (and probably are if you represent clients in the healthcare industry) is the Health Insurance Portability and Accountability Act ("HIPAA"). HIPAA is a federal law that safeguards protected health information held by covered entities, such as healthcare providers, health plans, and healthcare clearinghouses. HIPAA regulates the use, disclosure, and security of protected health information, aiming to protect patient privacy and maintain the integrity of healthcare.

The Gramm-Leach Bliley Act of 1999 ("GLBA") is a federal law that applies to financial institutions.[39] GLBA requires financial institutions to provide privacy notices to consumers, explain how customer information is collected and shared, and implement safeguards to protect customer data.[40]

The Children's Online Privacy Protection Act ("COPPA") is a federal law that safeguards the privacy of children under the age of 13.[41] COPPA imposes requirements on website operators and online services to obtain parental consent for the collection and use of personal information of children.[42]

[39] 15 U.S.C. §6801 *et seq*. (2023).

[40] *Id.*

[41] 15 U.S.C. §§6501-6506 (2023).

[42] *Id.*

B. FOREIGN REGULATION

In June 2023, the European Parliament passed the text of the Artificial Intelligence Act ("AI Act").[43] The new law, which would apply to the European Union ("EU), establishes obligations for providers and users depending on the level of AI risk. The law will take effect two years after the EU countries in the Council agree on the final version of the law. The grace period allows companies to adapt gradually and prepare for the changes until the rules come into force.

The AI Act identifies "unacceptable risks," which are AI systems that pose a significant threat to people. These include: cognitive behavioral manipulation of people or specific vulnerable groups (*e.g*., voice activated toys encouraging dangerous behavior in children); social scoring; and real time and remove biometric identification systems, such as facial recognitions. With some exceptions, these systems are banned in the EU.

The AI Act law also identifies "high risk" AI systems that negatively affect safety or fundamental rights. High risk AI systems fall into two categories. The first is AI systems that are used in products falling under the EU's product safety regulation (*e.g*., toys, aviation, cars, medical devices, elevators0. The second is AI systems that fall into eight specific areas, such as biometric identification and categorization of natural persons, law enforcement, education, and vocational training. These systems must be registered in an EU database.

[43]EU AI Act: first regulation on artificial intelligence, News European Parliament, https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence#:~:text=It%20says%20that%20AI%20systems,world's%20first%20rules%20on%20AI (Aug. 6, 2023). *See also Artificial Intelligence Act*, Briefing, EU Legislation in Progress, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

The AI Act regulates generative AI, like ChatGPT. These type of systems must comply with transparency requirements, such as disclosing the content generated by AI, designing the model to prevent it from generating illegal content, and publishing summaries of copyrighted data used for training.

The AI Act identifies "limited risk" AI systems. These systems must comply with minimal transparency requirements that would allow users to make informed decisions.

The EU also has enacted the General Data Protection Regulation ("GDPR"), which is the toughest privacy and security law in the world. Although it was drafted and enacted in the EU, it imposes obligations into organizations anywhere, so long as they target or collect data related to people in the EU.[44]

The GDPR sets forth rules regarding the processing and sharing of personal data for the protection of natural persons.[45] If you process data, you have to do so in accordance with seven protection and accountability principles outlined in Article 5.1-2.[46] These seven principles include: (1) lawfulness, fairness, and transparency; (2) purpose limitation; (3) data minimization; (4) accuracy; (5) storage limitation; (6) integrity and confidentiality; and (7) accountability. It also sets out severe remedies in the case of non-compliance.[47] The GDPR applies to all phases of AI, from the development of the AI system and its training with personal

[44] *What is GDPR, the EU's new data protection law?*, https://gdpr.eu/what-is-gdpr/ (last accessed Sept. 20, 2023).

[45] *Id*.

[46] *Id*.

[47] *Id*.

data to its implementation for data analytics and decision-making. This is one of the areas where we can help clients.

C. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

The National Institute of Standards and Technology ("NIST") is a federal agency that promotes and advances measurement science, standards, and technology. In collaboration with private and public sectors, NIST has developed a framework to better manage risks to individuals, organizations, and society associated with AI.[48]

On January 26, 2023, NIST released the first version of the AI Risk Management Framework ("AI Framework 1.0") and companion papers.[49] The AI Framework was developed through a consensus-driven, open, transparent, and collaborative process. Two months later, on March 30, 2023, NIST released the "Trustworthy and Responsible AI Resource Center," which facilitates the implementation of, and international alignment with, the AI Framework.

AI Framework 1.0 contains a comprehensive discussion on how organizations can frame risks related to AI and intended audience.[50] The document analyzes AI risks and trustworthiness, "outlines the characteristics of trustworthy AI systems, which include valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy enhanced, and fair with their harmful biases managed."[51]

---

[48] NIST, AI Risk Management Framework | NIST (last accessed Sept. 22, 2023).

[49] NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0) (nist.gov) (last accessed Sept. 22, 2023).

[50] NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0) (nist.gov) at 1.

[51] *Id.*

D. FDA DRAFT GUIDANCE

For those practicing medical device and healthcare law, you should be familiar with FDA's ongoing role in AI. On April 3, 2023, FDA released a draft guidance document called "Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence/Machine Learning (AI/ML) – Enabled Device Software Functions" ("FDA Draft Guidance"). [52] The purpose of the FDA Draft Guidance is to further develop a regulatory approach tailored to AI and ML-enabled devices in order to protect and promote public health. The document describes machine learning-enabled device software functions ("ML-DSFs"), which have become an important part of many medical devices.

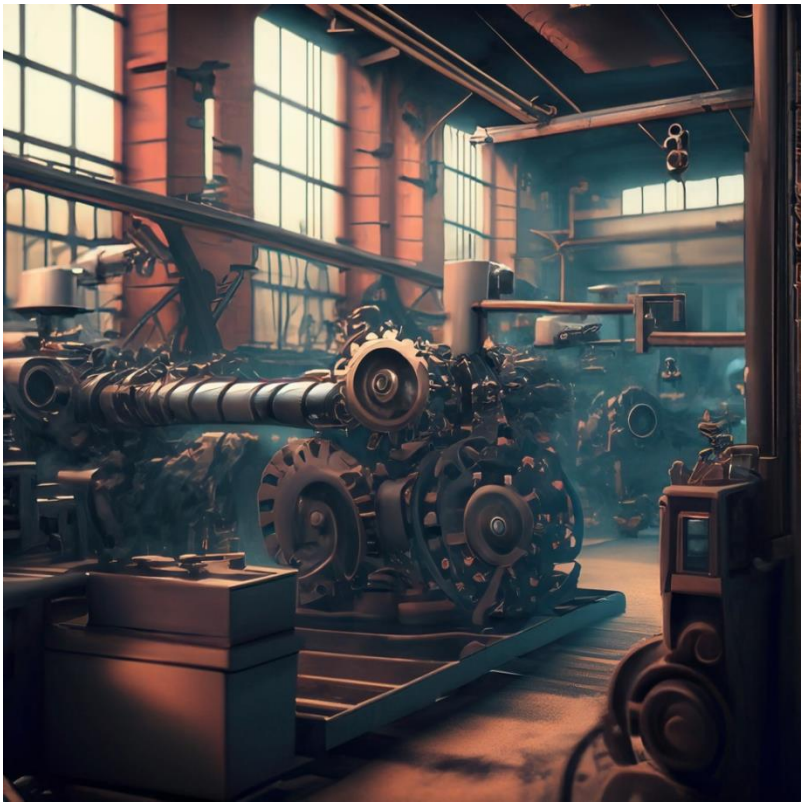
FDA's draft guidance "proposes a least burdensome approach to support iterative improvement through modifications to an ML-DSF while continuing to provide a reasonable assurance of device safety and effectiveness."[53] The document provides recommendations on the information to be included in a Predetermined Change Control Plan (PCCP) provided in a marketing submission for an ML-DSF. It "recommends that a PCCP describe the planned ML-DSF modifications; the associated methodology to develop, implement, and validate those modifications; and an assessment of the impact of those modifications."[54] FDA reviews the PCCP as part of a marketing submission to ensure the continued safety and effectiveness of the device "without necessitating additional marketing submissions for implementing each

[52] FDA Draft Guidance, https://www.fda.gov/media/166704/download.

[53] *Id.* at 2.

[54] *Id.*

modification described in the PCCP."[55] While only in draft format at this time, the FDA Draft Guidance provides insight into the FDA's through process in handling ML-DSFs, which is useful for our industry clients.



VI. PROTECTING YOUR CLIENTS (AND YOUR FIRM)

No lawyer can ignore the impact of AI. Having a working understanding of AI falls within the duty to provide competent legal representation. How you protect your client will depend, in part, upon your client's business. For example, if you represent manufacturers of medical devices using ML-DSF components, then you will need to familiarize yourself with the FDA discussions and draft guidelines. If you represent clients who conduct business in the EU, then you will need to understand the laws in the EU. If you use AI tools in your legal practice,

[55] *Id.*

then you will need to implement a plan to protect confidential client information and minimize the risks of data and security breaches, among other things.

What does competent representation look like with the evolution of AI in our clients' businesses and in your legal practices? New York and California interpret the duty of "competent representation" to include "competent in the use of technology that is critical to the lawyer's representation".[56] Florida requires professional responsibility rules include competence in technology and continuing legal education in an approved technology program.[57] Irrespective of what state you practice in, a best practice is for lawyers to associate with or retain a non-lawyer advisor with established technological competence in the relevant field. Also, lawyers should be generally aware of the developments in the AI world applying to their clients and legal practice through continuing legal education.

If your law practice uses AI tools, then you should consider creating guidelines on best practices to safeguard confidential communications and work product. Data stored on a public AI platform may not be secure. Service providers, AI engineers and AI technicians can access

---

[56]NYCLA Formal Op. 749 (Feb. 21, 2017) (a lawyer has duty of technological competence to the extent that technology is pertinent to a representation, and can fulfill this duty if the lawyer possesses the requisite knowledge personally, acquires the requisite knowledge before performance is required, or associates with one or more persons who possess the requisite technological knowledge); California Standing Committee on Professional Responsibility and Conduct Formal Op. 2015-193: (lawyer's obligations under the ethical duty of competence evolve as new technologies develop and become integrated with the practice of law). For more information *see* James Walker, *Cybersecurity, Encryption and Emergency Technology and the Duty to Protect a Client's Confidential Information*, 20191017P NYC Bar 87 (2019).

[57]*In re Amendments to Rules Regulating the Florida Bar 4-1.1 and 6-10.3*, 200 So.3d 1225, 1225-1226 (Fla. 2016). The Florida Supreme Court held that "the comment to rule 4-1.1 (Competence) is amended to add language providing that the competent representation may involve a lawyer's association with, or retention of, a non-lawyer advisor with established technological competence in the relevant field." *Id.* at 1226. The Court also amended rule 6-10.3 to require continuing legal education in "approved technology programs". *Id.* The version of rule 6-10.3, which takes effect on January 8, 2024, requires at least 3 of the 30 continuing legal education credits required every three years to be in "approved technology problems". F.S.A. Bar 6-10.3 (as amended).

the prompts, data, and written product to improve their systems.[58] One article provides the following considerations for lawyers when using AI tools: focus on maintaining privacy; be cautious when entering prompts on AI tools; clearly mark generated content as privileged; and always review the generated content to stay within the scope of privilege.[59]

VII. CONCLUSION

This is just the beginning of the conversation on AI and its impact on clients and legal practice. Like a good movie franchise, there will be sequels.

[58] Antonious Sadek, *et al.*, *How to Protect Atty-Client Privilege While Using Generative AI*, Law 360 (Sept. 21, 2023).

[59] *Id.*