Reuters Legal News

Artificial intelligence and trade secrets

By R. Mark Halligan, Esq., FisherBroyles LLP

DECEMBER 11, 2023

Generative artificial intelligence (AI) is an emerging class of machine learning technology that can synthesize content including text and images. This article outlines the history of generative artificial intelligence and the serious risk of trade secret forfeiture emanating from AI tools.

The name ChatGPT is an acronym for "Generative Pre-Trained Transformer". It is an AI tool created by OpenAI, that *responds* to an input unlike a search engine that only *returns* results on the internet. This revolutionary technology communicates like a human and can contextualize inputs to create texts, lyrics, poems, programming codes and many other outputs being discovered daily.

In March 2023, OpenAI released GPT-4 which advances the core technology of ChatGPT by enabling the chat software to solve more difficult problems with greater accuracy, It also adds new capabilities such as accepting images as inputs and generating captions, classifications, and analyses. GPT-4 can also handle over 25,000 words of text, allowing long-form content creation, extended conversations, and document search and analysis.

Today, generative artificial intelligence produces results without explaining why or how the processes work.

The history of the creation of Chat GPT is important. The original chatbot was created by MIT computer scientist Joseph Weizenbaum in 1966 and named ELIZA. The next development was a large language model (LLM) that is a machine-learning neuro network trained through input/output sets. Information is ingested, or content entered, into the LLM and the output is what the algorithm predicts the next word will be.

Today, generative artificial intelligence produces results without explaining why or how the processes work. Training LLMs to use the right data requires the use of massive server farms and supercomputers. ChatGPT is an example of an LLM that was initially trained to predict the next word in a sentence and other autocompletion tasks.

There are many issues relating to generative AI models. For example, computer scientists have discovered that an LLM might be trained in one programming language but then generates code in another programming language it has never seen before. Often, there are incorrect answers.

Another concern is AI is too eager to please. If AI doesn't have enough actual information in its knowledge base, it fills in gaps with stuff that sounds like it could be correct according to its algorithm.

Using a generative artificial intelligence system with input/output trade secrets will destroy the trade secrets because there is no confidential relationship that can exist between a person and a computer.

There is an element of randomness in generative AI systems that involve trillions of variables that make it difficult or impossible to dissect how the generative AI system arrives at a particular output. There are so many layers of machine-learning algorithms that a human can no longer go into the code and trace exactly why the software made the choices it did.

AI can lie. A generative AI model cannot tell you whether something is factual; it can pull data only from what it's been fed. So if that data says that the sky is green, the AI will give you back stories that take place under a lime-colored sky.

There is also the phenomenon of AI hallucination. If a user makes a request of a generative AI tool, the user desires an output that appropriately addresses the prompt (i.e., a correct answer). However, sometimes AI algorithms produce outputs that are not based on training data, are incorrectly decoded by the transformer or follow no identifiable pattern. In other words, it "hallucinates" the response. Another concern is AI bias which is an anomaly in the output of machine learning algorithms due to the prejudiced assumptions made during the algorithm development process or prejudices in the training data.

AI's capabilities are not static and continue to expand exponentially as the technology advances. The complexity of AI models has been doubling every few months. Artificial Intelligence systems' capabilities remain undisclosed even to their inventors. AI systems

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner. Nothing in this publication should be construed as legal advice or creating an attorney-client relationship. The views expressed in this publication by any contributor are not necessarily those of the publisher.

THOMSON REUTERS®

are building new capacities without understanding their origin or destination.

Protecting trade secrets requires that reasonable measures be taken to protect the secrecy of trade secret information. An unprotected disclosure of a trade secret to a third party vitiates the status of the information as a trade secret.

Generative artificial intelligence is built upon inputs and outputs. The way an AI system is designed, the received inputs become outputs. So if Company A inputs a request for the Product X formula, the output will be something that no longer qualifies as a trade secret because the AI system is not designed to differentiate between confidential and non-confidential information. The input will not qualify as a trade secret, and the output will not qualify as a trade secret, and future inputs or outputs of the Product X formula will not qualify for trade secret protection.

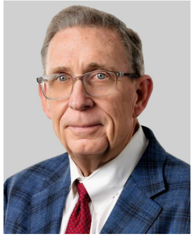
In order to protect a particular piece of information as a trade secret, the receiving party must make an express promise of confidentiality before the disclosure of the trade secret. This cannot happen using a generative AI system because the receiving party is not a person.

Alternatively, if the particular piece of information is disclosed to the receiving party under circumstances where the receiving party knew or had reason to know that the disclosure was intended to be kept confidential — the same result occurs if the receiving party is a generative AI system. There is no protection because the receiving party is not a person. Instead, the status of the information as a trade secret is vitiated for the unprotected disclosure to a third party.

Trade secrets are fragile assets. A trade secret once lost is lost forever. Using a generative artificial intelligence system with input/output trade secrets will destroy the trade secrets because there is no confidential relationship that can exist between a person and a computer. Only a blanket ban against the use of generative artificial intelligence tools would protect trade secrets.

R. Mark Halligan is a regular contributing columnist on trade secrets law for Reuters Legal News and Westlaw Today.

About the author



R. Mark Halligan is a partner at **FisherBroyles LLP** and is based in Chicago. He focuses his practice on intellectual property litigation and is recognized as a leading practitioner in the development of automated trade secret asset management blockchain systems. He teaches Advanced Trade Secrets Law in the LLM program at University of Illinois Chicago School of Law and is the lead author of the "Defend Trade Secrets Act Handbook," 3rd Edition, published by Wolters Kluwer. He can be reached at rmark.halligan@fisherbroyles.com.

This article was first published on Reuters Legal News and Westlaw Today on December 11, 2023.