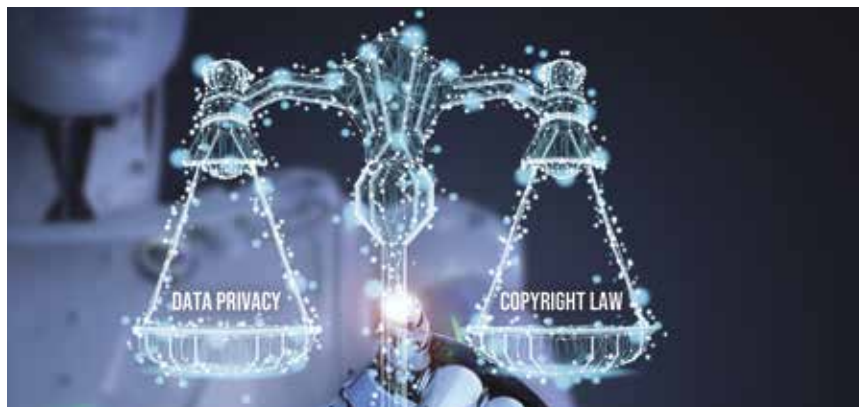


Artificial Intelligence versus Copyright Protections and Data Privacy

By Judge Herbert B. Dixon Jr.



The capabilities of artificial intelligence (AI) applications are advancing at a rapid pace. In February 2023, the Annual Threat Assessment of the U.S. Intelligence Community stated that new technologies, explicitly referencing AI, “are being developed and are proliferating faster than companies and governments can shape norms, protect privacy, and prevent dangerous outcomes.”¹ In October 2023, emphasizing the urgency of considering the national importance of the topic, President Joseph Biden issued an all-encompassing Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence. The Whitehouse issued a fact sheet about the Executive Order stating, “Without safeguards, AI can put Americans’ privacy further at risk. AI not only makes it easier to extract, identify, and exploit personal data, but it also heightens incentives to do so because companies use data to train AI systems.”²

Understandably, significant issues have arisen from the availability and use of AI. These issues include the need and extent for regulation of AI applications, the admissibility of evidence created by artificial intelligence, the ownership of AI-produced products, national security, AI bias, and more. For this technology column, I identify two hotly debated issues arising from the development and use of Generative Artificial Intelligence (GenAI), a specific form of AI. The issues are copyright protection and data privacy.

What Is Generative Artificial Intelligence (GenAI)?

There is not a single definition of GenAI.

The fact that GenAI is a type of artificial intelligence is evident by its name. GenAI is a form of artificial intelligence capable of generating text, images, and videos through learning patterns from pre-existing data.³ The GenAI applications with which the public is most familiar are:

- **Chatbot:** An AI application that simulates human-like responses to questions, inquiries, and directives.
- **Image generator:** An AI application that generates images in response to a directive or “prompt.”
- **Video generator:** An AI application that generates a video in response to a directive or “prompt,” often called a deepfake.
- **Voice clone:** An AI application that generates speech and voice sounds, sometimes called an audio deepfake.⁴

This technology column intends to briefly identify the primary allegations of copyright infringement and data privacy violations resulting from the development and use of GenAI applications.

The GenAI Chatbot

What the public has learned from the use of chatbots is that, with minimum information input by the user, the application produces a remarkable, authentic-sounding, and sometimes seemingly comprehensive response. Directives or questions to chatbots range from whimsical to substantive, such as, “Write a poem about the Library of Congress”; “Write a small claims complaint against xyz repair shop that failed to fix my car correctly”;

“Write a congratulatory note [or speech] to celebrate my nephew’s college graduation [or marriage, or first home sale as a real estate agent, or other accomplishment]”; “Write a paragraph for a legal brief that compares plausibility pleading under *Twombly* and *Iqbal* in U.S. Federal Courts to the notice pleading standard articulated in *Conley* that has been adopted in most state courts. Provide citations to appropriate legal authority in Bluebook format”; “Write an opening paragraph to a judicial opinion about cats suing dogs”;⁵ “Write an essay on [choose your topic]”; “What is my illness if my symptoms are sneezing, runny nose, sore throat, and headache?”; etc. The question or request a person might submit to a chatbot is limited only by the person’s imagination. The most well-known chatbots are ChatGPT, Bing, and Bard.



Judge Herbert B. Dixon Jr. is a senior judge with the Superior Court of the District of Columbia. He is chair of the *ABA Journal*

Board of Editors, a former chair of both the National Conference of State Trial Judges and the ABA Standing Committee on the American Judicial System, and a former member of the Techshow Planning Board. You can reach him at Jhbdixon@gmail.com. Follow Judge Dixon on X (formerly known as Twitter) @Jhbdixon.

How Chatbot Creators Train Their Applications to Give Coherent and Human-Sounding Responses

General-purpose chatbots such as ChatGPT, Bing, and Bard are trained on massive datasets, typically called large language models (LLMs). The training data come from almost every source imaginable, including the internet and other public and nonpublic material sources. Based on the training data, chatbots are trained to recognize language and generate a response by predicting the next most likely word or phrase as it delivers its response. As an example, if someone asked a chatbot to predict the next word in the phrase, “buckle my . . . ,” it might choose the word “shoe” based on the nursery rhyme that begins “one, two, buckle my shoe.” However, depending on the dataset on which the model was trained, there may be instances after the phrase “buckle my” in which the word “belt” occurs most often, in which case the chatbot would finish the phrase with the word “belt.”

As an example of the vast amount of data on which a chatbot is trained, the Congressional Research Service reports that the LLM on which ChatGPT was trained contained over 45 terabytes of text data “scraped” from the internet, including Wikipedia and digitized books. Further, the ChatGPT-3 models had over 175 billion parameters—variables used by the model to process and understand the training data.⁶ The parameters guide the model to provide coherent (hopefully accurate) and human-like responses. However, when I asked ChatGPT about its training data and parameters, it responded as if it were guarding proprietary information, stating:

As an AI language model, I don't have access to specific details about the training data or the exact number of parameters used in ChatGPT-4. However, I can tell you that models like ChatGPT-4 are typically trained on large-scale datasets consisting of diverse text sources from the internet. The training process involves millions or even billions of text samples to help the model learn patterns and generate responses. The number of

parameters in a model can vary, but it is typically in the range of hundreds of millions to billions.

Well said, ChatGPT—spoken like a well-trained company spokesperson.

Copyright Protection Concerns

Numerous authors, writers, journalists, and playwrights contend that the datasets of LLM models are trained on massive amounts of their writings without the consent or compensation of the content creator or rightful owner. More specifically, the claimants allege that AI developers have misused their writings by copying their works without permission to train the artificial intelligence–powered chatbots to respond with human-like responses.⁷ Several content creators have filed lawsuits seeking an injunction against future use and compensation for the unauthorized use of their works.

Among those alleging improper use of their data are the *Washington Post*, the *New York Times*,⁸ and other prominent news publications, some of which have installed a blocker that prevents their content from being collected and used to train ChatGPT.⁹ To resolve what they claim are improper uses of their data, several publication entities and news outlets are negotiating with chatbot creators to license the use of their materials. They claim the chatbots are becoming direct competitors with the newspapers by creating responses based on the original reporting of the newspapers' journalists and writers.¹⁰ If these negotiations are unsuccessful, it is widely assumed that the next step will be more litigation alleging improper use of copyrighted materials. Most experts agree that judicial determinations will resolve whether AI platforms are committing some form of copyright infringement or whether the use of those materials falls within the fair use doctrine, which would not be a violation of the copyright laws.

Data Privacy Concerns

When considering the term “data privacy,” think broadly to include the concepts of client confidentiality. Not only is it possible that a chatbot may compromise

private individual information revealed by an individual in a blog, on social media, or in a chatbot inquiry, but the chatbot may also acquire confidential information about an individual from input or postings by a lawyer or other professional who has a duty of confidentiality to that individual. As mentioned, LLM training datasets are created by acquiring information from numerous sources. That information might include names, addresses, phone numbers, financial and medical information, and more, which the chatbot might reveal in response to another person's inquiry. Currently, the major chatbots are trained to respond negatively when queried about a person's private information. However, it is only a matter of time until a bad actor, a less sophisticated chatbot, or a “glitch” causes the sharing of private or personal information. A paper produced following research by academic and industry experts reports that sensitive data and personal information from datasets can be extracted from or revealed by the datasets on which some LLMs have been trained.¹¹

Claims of improper use of personal data are not confined to the United States. For example, the Italian Data Protection Authority briefly banned OpenAI from operating in Italy in response to complaints that OpenAI unlawfully collected users' data and failed to prevent underage users from accessing inappropriate material. OpenAI resumed its services for users in Italy after it “addressed or clarified” the issues the Italian Data Protection Authority raised. In addition, OpenAI is facing more challenges based on reports that Spain, Canada, and other countries have opened or considered opening investigations into its practices, including how it collects training data for its large language model and what information that model produces for users.¹²

As this column was being finalized and submitted for printing, a federal lawsuit seeking class action certification was filed in the Northern District of California against OpenAI, the creators of ChatGPT. The lawsuit alleges that the AI company violated the copyrights and privacy of millions of internet users to train their AI platform

when it used data scraped from the internet to train its software, including social media comments, blog posts, Wikipedia articles, and family recipes. This is another instance of litigation to watch that may provide some answers to the hotly debated issues arising from the creation and use of chatbots.

Final Thoughts

The extraordinary developments in AI capabilities have been transformative. As with other transformative inventions, issues have arisen regarding their effects on society. Because the training data on which AI chatbots are trained come from vast sources, AI developers should ensure that they are in compliance with the law regarding their acquisition of data used to train their models. Concurrently, users should be concerned not only about the accuracy of responses they receive from AI chatbots, but also about the confidentiality of the information they input to AI

platforms and whether the responses they receive are subject to copyright or privacy restrictions. No less than with other transformational technological advancements throughout history, AI is also suffering growing pains. Fear not; I am confident the future will present even more challenges with each new transformational technological advancement.

Endnotes

1. OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 26 (Unclassified Report) (Feb. 6, 2023), <https://bit.ly/3QCHddw>.

2. Press Release, White House, Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence (Oct. 30, 2023), <https://bit.ly/3svukKj>.

3. CONG. RSCH. SERV., GENERATIVE ARTIFICIAL INTELLIGENCE AND DATA PRIVACY: A PRIMER, NO. R47569 (May 23, 2023), <https://crsreports.congress.gov/product/pdf/R/R47569>.

4. *Id.*

5. Christopher Michael Malikschratt, *The Real Future of AI in Law: AI Judges*, LAW TECH. TODAY, Oct. 18, 2023, <https://bit.ly/3FZAKOo>.

6. CONG. RSCH. SERV., *supra* note 3.

7. Blake Brittain, *More Writers Sue OpenAI for Copyright Infringement over AI Training*, REUTERS (Sept. 11, 2023), <https://bit.ly/3SGG8CN>.

8. Bobby Allyn, "New York Times" Considers Legal Action Against OpenAI as Copyright Tensions Swirl, N.Y. TIMES (Aug. 16, 2023), <https://bit.ly/40DpKWO>.

9. Nitasha Tiku, *Newspapers Want Payment for Articles Used to Power ChatGPT*, WASH. POST (Oct. 20, 2023), <https://bit.ly/3SFSTi4>.

10. Allyn, *supra* note 8.

11. Nicholas Carlini et al., *Extracting Training Data from Large Language Models*, ARXIV (June 15, 2021), <https://arxiv.org/abs/2012.07805>.

12. Adi Robertson, *ChatGPT Returns to Italy After Ban*, THE VERGE (Apr. 28, 2023), <https://bit.ly/3MleZwM>.