Westlaw Journal

COMPUTER & INTERNET

Litigation News and Analysis • Legislation • Regulation • Expert Commentary

VOLUME 41, ISSUE 12 / OCTOBER 18, 2023

WHAT'S INSIDE

EXPERT INTERVIEW

Q&A: Privacy expert Jamie N. Nafziger on risks posed by AI tech

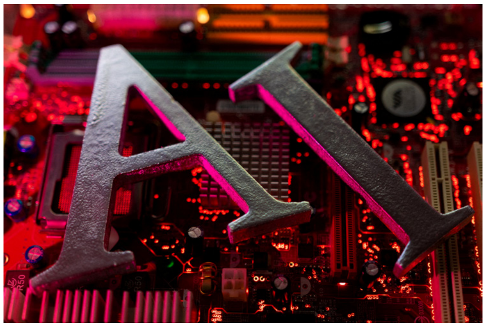
By Patrick H.J. Hughes

Dorsey & Whitney LLP partner Jamie N. Nafziger offers insights on the impending legal issues surrounding artificial intelligence technology.

Consumer class actions against OpenAI have surfaced in California courts in recent weeks, with allegations that say artificial intelligence programs are stealing personally identifiable information "from hundreds of millions of internet users."[1]

Commentators have noted the apparent threats AI poses to people's privacy, but what activities are actionable in court mostly remain to be seen with respect to ChatGPT and other large language models.

Dorsey & Whitney LLP partner Jamie N. Nafziger is on the cutting edge of digital technology development, with knowledge of AI as well as ever-changing privacy laws and internet regulations. Her experience helping clients comply with the California Consumer Privacy Act,



REUTERS/Dado Ruvic

CONTINUED ON PAGE 11

EXPERT INTERVIEW

Q&A: Domain Days Dubai — introducing domain professionals to the Middle East

By Patrick H.J. Hughes

Domain Days Dubai's founder and curator, Munir Badr, discusses why domain professionals from all over the world are coming to Dubai for a one-of-a-kind, domain-centric idea exchange.

Domain Days Dubai 2023 will be held Nov. 1 and 2 in — as the name implies — Dubai, the most populous city in the United Arab Emirates and the region's reputed technology hotspot.

The first of its kind, the event is intended to connect domain investors, registrars, intellectual property attorneys and anyone involved in the web industries with their counterparts in the Middle East and North Africa while providing educational opportunities about digital developments in the MENA region.

CONTINUED ON PAGE 13

AI tech

CONTINUED FROM PAGE 1

numerous other federal and state privacy laws, and the European Union's General Data Protection Regulation has made her a valuable resource to prepare for the AI disputes to come.

Westlaw Today tapped Nafziger's legal knowledge to better understand some of the issues behind what could amount to a deluge of litigation over AI.

Westlaw Today: In a recent suit against OpenAI and Microsoft, the plaintiffs say AI technology has "systematically scraped 300 billion words from the internet." Is this a fair assessment? And if so, is this practice new?

Jamie N. Nafziger: This is a fair assessment and likely represents an undercount of the billions of words on which AI technology has been trained. OpenAI claims that it developed ChatGPT mainly using three sources of information: (1) publicly available information on the internet, (2) information licensed from third parties, and (3) information provided by users and human trainers. Scraping publicly available information from the internet is not new — it has been happening almost as long as the internet has been used by the public.

Companies have sued others over scraping their websites for data for over 20 years based on a number of different legal theories. Over the years, trespass to chattels, violation of the Computer Fraud and Abuse Act, and breach of contract were some of the most common scraping-related causes of action. In recent years, the law has been disrupted by the U.S. Supreme Court, which adopted a narrow interpretation of the Computer Fraud and Abuse Act in *Van Buren v. U.S.*,[2] and by 9th Circuit decisions in the *hiQ Labs Inc. v. LinkedIn Corp.* case.[3]

Another important set of recent scraping cases includes the numerous lawsuits and regulatory actions taken against Clearview AI, which scraped photos from popular websites, ran facial recognition software on them, and sold access to its databases to corporations and government agencies. Clearview AI's software was considered illegal in numerous jurisdictions, and it faced several significant lawsuits, including one by the ACLU, which settled last year.

WT: OpenAI has also been accused of rushing its AI products to market to take advantage of the potential to make immediate profits. What are some examples of safeguards that those developing AI technologies should take to avoid legal liability?

JNN: Launching AI technologies raises a host of complex legal issues. The main legal risks fall into the areas of intellectual property, privacy, torts based on errors or bias, and security breaches/criminal activity. Those developing AI technologies can take steps to reduce their liability risk in all of these areas. For instance, in the intellectual property area, they should ensure that they train their models on information to which they have legal access, such as through licensing, and should review the recent scraping case law carefully. AI companies are facing numerous lawsuits by authors and artists regarding copyright infringement. In addition, the current strike in Hollywood is based in part on writer and actor concerns about AI. AI companies should monitor these cases closely and be prepared to adapt training and output systems, if needed.

In connection with privacy, AI companies should consider deleting personal information from their training sets, designing their technology in a way that would allow them to remove or correct information about a person upon request, and taking special care in connection with sensitive personal information such as children's information, health information and financial information. Some of the newer state privacy laws require opt-in consent in connection with the collection of certain personal information. Opt-in consent will be difficult to obtain in connection with training of systems on existing databases, so this raises a sizable risk. AI companies should have an easier time seeking opt-in consent from users and should implement systems to obtain and document consent from users and to respond to rights requests from users.

The potential benefit of AI systems is tremendous.

Errors and bias in AI systems present significant legal risk for AI companies. A number of defamation cases have been brought based on AI hallucinations, and federal agencies have made clear that they will pursue legal action in connection with bias in AI systems. Thus, it is worth devoting serious attention to the prevention of errors and bias in AI systems. These efforts should cover all aspects of the system from the data on which the system is trained, to filters that block biased responses in text, to testing of ranking and sorting systems to make sure they do not output biased results. I expect this will be one of the areas where we will see the greatest action by state and federal prosecutors and government agencies.

Finally, unfortunately, AI art systems are being used by criminals including child pornographers. AI systems should become familiar with the legal requirements in connection with child pornography, such as reporting to the CyberTipline, and should set up systems both to prevent their systems from being used in this way and to find, remove and report such uses when they occur.

WT: The suit against OpenAI and Microsoft also alleges "a nontrivial number of experts" claim AI has created "risks to humanity" that are even greater than the threat posed by the Manhattan Project's creation of nuclear weapons. As an expert in these matters, would you say this is a fair assessment or is this statement overblown?

JNN: This is a fair assessment and should be a top priority. Generative AI systems have not yet reached the level of artificial general

Jamie N. Nafziger is a partner at **Dorsey & Whitney LLP** in Minneapolis and chairs the firm's cybersecurity, privacy and social media practice group. She has more than 25 years of experience as a technology lawyer with a focus on helping clients launch cutting-edge online services and mobile apps and advertise their products and services in compliance with privacy, trademark, and a host of online and advertising laws. She is a frequent writer and speaker on privacy, artificial intelligence, mobile apps, trademark law, internet law, social media and domain names. She has been named one of the Top 250 Women in IP and a BTI Client Service All-Star MVP. She can be reached at nafziger.jamie@dorsey.com.

intelligence where they can match or surpass human intelligence, but even the existing generative AI systems raise risks. This is especially true when generative AI systems are connected to devices in the Internet of Things or given the opportunity to interact outside of their own platform. For instance, when ChatGPT-4 was being released, OpenAI released a report on the "Potential for Risky Emergent Behaviors" which described testing where GPT-4 was asked to solve a CAPTCHA and ended up hiring a human to solve it. In the process, GPT-4 lied and claimed that it was a person with a visual impairment. If we extend that type of "behavior" to an AI system running military equipment, we can see the potential for deadly trouble.

> Some bad actors are using AI to make their scams and hacks more convincing.

On the other hand, the potential benefit of AI systems is tremendous. We could use it to find cures for diseases, make society run more efficiently, reduce human errors, and for all sorts of beneficial purposes we cannot yet envision. Thus, in my view, the potential benefits make it worth working to avoid the worst-case scenario without scrapping the technology.

WT: A primary concern with the introduction of new AI systems has been the potential that unauthorized entities might gain access to private information through data breaches or accidental leaks. Should AI developers be extra careful to avoid hackers?

JNN: Both AI users and AI developers should be careful about this. In public AI systems, individual users should not be uploading or disclosing sensitive personal information such as their financial or health information. As more and more companies are acquiring access to use AI systems within closed environments such as a workplace, more sensitive information will be uploaded into AI systems. To protect that information, companies should negotiate strong agreements regarding security with AI systems, and AI systems should develop very secure platforms to avoid data breaches. Unfortunately, some bad actors are using AI to make their scams and hacks more convincing and to develop malware.

WT: Reports of hallucinations have been common. Is there potential for any misinformation to result in litigation against AI companies? How about AI users?

JNN: Yes. Lawsuits have already been filed against AI companies based on hallucinations. Other damaging hallucinations have also been reported, and this area seems ripe for litigation. One case involves a pro-gun radio talk show host who sued OpenAI for defamation after ChatGPT allegedly falsely accused him of embezzling money from a pro-gun group. Other reports have involved hallucinations regarding false allegations of sexual assault against law professors and false claims about elected officials. Although hallucinations are common, it is unclear whether these lawsuits will be able to survive motions to dismiss. I have not heard about litigation against other users. However, I imagine it is theoretically possible that one user could provide lots of false information about someone to an AI system with the training setting enabled such that the system would begin presenting false information about the target and the target could sue the other user.

WT: The European Commission has announced that the world's first comprehensive legal framework for artificial intelligence is being developed for the European Union. Canada is developing similar legislation. To your knowledge, in what ways will these acts address privacy concerns?

JNN: Canada had proposed the Artificial Intelligence and Data Act as part of its proposed privacy amendments in Bill C-27. The act was tabled in June 2022. If passed, it would require AI systems to assess whether they constitute high-impact systems (pursuant to regulations that have not been developed) and would seek to protect people from biased outputs and from harm caused by AI systems. Whether this bill or another will be reintroduced in Canada is unknown. However, like several federal agencies in the U.S., Canada has committed to enforcing existing laws and regulations against AI systems. In May 2023, it announced that it is investigating OpenAI's data collection and usage. In August, it announced that it is working on a Generative AI Code of Practice.

The EU's Artificial Intelligence Act is not yet in force (and likely will not be until at least late 2025). However, under the act, AI systems are divided by risk level, and each level has different requirements in connection with protecting personal information. AI systems that constitute an unacceptable risk are banned. Those that constitute a high risk such as resume scanning applications that rank applicants are subject to strict legal requirements such as risk assessment and mitigation, logging, traceability and human oversight. Limited risk applications must meet transparency requirements, and minimal risk applications will not be subject to regulation. The tricky part of moving forward with the AI Act is determining which types of AI applications fit within each risk level. That is the subject of ongoing negotiations in the EU now. Ultimately, privacy concerns will likely be addressed by the AI Act in that AI applications that cause the most serious privacy risks will be either banned or regulated.

NOTES

[1] *A.T. v. OpenAI LP*, No. 23-cv-4557, *complaint filed* (N.D. Cal. Sept. 5, 2023).

[2] 141 S. Ct. 1648 (2021).

[3] 938 F.3d 985 (9th Cir. 2019) and 31 F.4th 1180 (9th Cir. 2022).