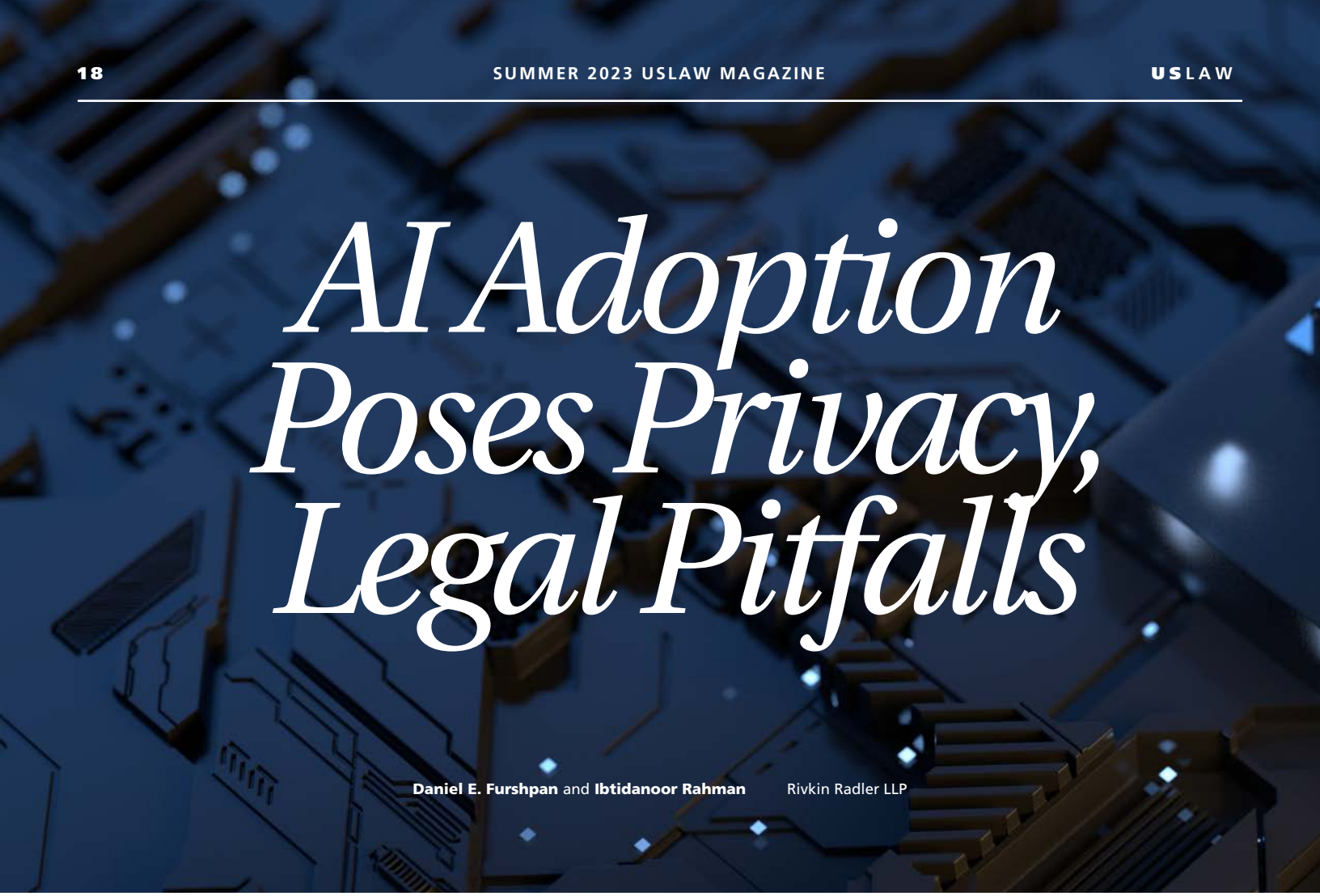

AI Adoption Poses Privacy, Legal Pitfalls

Daniel E. Furshpan and **Ibtidanoor Rahman** Rivkin Radler LLP

Artificial Intelligence (AI) is a new technology that enables machines to perform tasks with human-like intelligence. Among the various AI programs that are available, ChatGPT is widely considered to be the most popular. For a relatively small fee, the program can answer questions and assist with tasks such as writing code, composing text and even creating works of art.

To use ChatGPT, the user enters a prompt in a text bar, such as a question or command, and the program provides a relevant and meaningful response. The program also has the capacity to analyze and interpret large amounts of data. This makes it a powerful tool for companies across industries to improve their operations and processes.

But with new technology comes new concerns of data privacy and security along with questions about how AI data should be preserved and used in litigation.

Importantly, ChatGPT and other AI programs are not confidential. AI data, including prompts, are stored in a digital library and used to generate automated responses to other users' inquiries. Furthermore, it is unclear exactly who has access to the digital library and whether that information and data can be accessed or sold to third-party developers or advertisers. This is the major concern for companies that input sensitive business or customer information into the programs.

AI programs are also vulnerable to cyberattacks, just like most other online platforms. On March 20, 2023, OpenAI, the developer of ChatGPT, reported that they found a bug in the program's source code that allowed users to view the chat history of active users. While they were fixing this problem, they discovered another issue with their server that exposed some users' personal information, including first and last names, email addresses, credit card types, and the last four digits of their credit cards. OpenAI fixed the issue shortly after it was discovered, but the damage was done.

It should also be noted that information generated by an AI program is not always accurate. OpenAI admits that the technology is still in a research phase and can produce wrong information. There have even been lawsuits brought over the inaccuracies generated by AI, including a defamation lawsuit brought by a government official as a result of ChatGPT providing inaccurate information about that person, and copyright infringement lawsuits over AI programs using copyrighted material in its training data.

Given these security and accuracy concerns, many companies are implementing policies governing how their employees use AI programs. For example, some companies have established guidelines for employees to follow when using AI in order to ensure that no sensitive company or customer information is entered. And companies are monitoring their employees' use of AI programs to ensure that they are being used in a safe and confidential manner. Some companies are restricting employee use of AI altogether. Companies are also raising cybersecurity awareness. The goal of these policies is to minimize the potential risks associated with AI and to maintain control over how the technology is used.

Another issue that arises with AI technology is how it plays out in litigation. Since AI is such a novel and quickly emerging industry, there appear to be no published court opinions regarding disclosure of AI data. Generally, in discovery, documents and electronically stored information (ESI) must be turned over if it is relevant and proportional to the needs of the case. Information entered into and generated by AI is likely to be considered ESI and subject to disclosure. Accordingly, users must be careful and calculated when using an AI program as the data may ultimately be turned over to an adversary in litigation and

have unintended, adverse consequences.

Admissibility of AI data in a trial setting presents another challenge. The trial judge serves as the gatekeeper, responsible for evaluating the admissibility of evidence, including ESI, and deciding whether the jury should be allowed to hear it. Courts consider the validity, authenticity and trustworthiness of ESI when deciding whether to admit it as evidence. In that respect, proponents of AI evidence at trial need to establish that it is authentic; for instance, does the AI program that generated the evidence produce the result that its proponent claims it does?

There are possibly endless challenges to the validity of data produced by an AI program. The program could have been designed with a bias; the people who were trained to use the program may not be properly qualified; the AI may not have been properly tested. Additionally, given the complex nature of AI technology, jury confusion is another factor that is considered. Lawyers who intend to offer, or challenge, AI evidence need to do the necessary work to explain how the AI system functions, how it produces its output, and how that output is relevant to the case.

Even further, the intentional or even inadvertent deletion of AI data could lead to spoliation sanctions. Spoliation is the destruction or alteration of evidence that could be relevant to a dispute. Penalties for spoliation include monetary fines, evidence preclusion, a negative inference instruction, or even struck pleadings. Deleting a chat history or enabling an automated deletion process after litigation is commenced could be considered destruction of ESI, even if accidental. As an example, in *Meta Platforms, Inc. v. Brandtotal Ltd.*, No. 20-cv-07182-JCS (N.D. Cal. May 27, 2022), a magistrate judge granted the plaintiff's motion for sanctions due to the defendant's failure to preserve relevant data. The defendant in the case used a logger tool to track the operation of its software products. Testimony revealed that relevant data was stored in the logger tool but was lost due to an automated deletion process. Although the defendant's actions were not intentional, the court granted the plaintiff's motion for discovery-related sanctions because the defendant failed to preserve the relevant data, and the data could not be duplicated or replaced.

To summarize, while AI technology can be very beneficial to companies in terms of efficiency and cost savings, it is important for organizations to be aware of the privacy risks that come with its use, especially as it pertains to the handling and protection of sensitive information. Organizations should stay up to date with data privacy regulations and best practices for data security to ensure they are safeguarding sensitive company and customer information. Additionally, AI technology will inevitably be used in litigation, and it is necessary for companies and attorneys alike to stay abreast of new rules and court decisions governing the disclosure and admissibility of AI data.

Daniel E. Furshpan is a partner in Rivkin Radler's Critical Incident Response, General Liability and Medical Malpractice Defense practices. He can be reached at (516) 357-3436 or Daniel.Furshpan@rivkin.com.

Ibtidanoor Rahman is a summer intern at Rivkin Radler.