The Texas Lawbook

Free Speech, Due Process and Trial by Jury

Corporate Policies on the Use of AI Tools: A Q&A with Yokogawa’s George Niño

August 24, 2023 | BY BRAD WEBER

ChatGPT is one of several popular tools powered by generative artificial intelligence technology that can produce convincing, human-like answers to almost any question. These AI tools generate new content — such as text, images, audio, video or computer code — through computer algorithms trained to learn patterns and relationships in large sets of input data.

While this exciting new AI technology is at the core of several useful applications, it is still developing and can provide inaccurate results. The use of these AI tools by companies also raises a number of legal, ethical, privacy and security risks. As a result, many companies recently have adopted or are considering corporate policies for the use of AI tools by their employees.

What You Need to Know

- Companies with policies that totally ban the use of AI tools run a significant risk that some employees will disregard the restrictions because they consider the AI tools to be critical to their work.
- An effective corporate policy on the use of AI tools should be clear and concise, listing certain uses of these tools that are strictly prohibited, such as uploading confidential company data, business partner data or personal information.
- The policy also should describe other uses of these AI tools, such as gathering competitive market data or summarizing publicly available documents, which are permitted if the employee follows the other provisions in the policy.
- Because AI tools can produce inaccurate or biased outputs, the corporate policy also should require employees to review all content created by these applications for accuracy and appropriateness before publicizing or disseminating the content.
- In addition, to help mitigate data privacy concerns, corporate policies on the use of AI tools should require employees to disable the chat history when using ChatGPT or enable the data privacy settings on other similar applications.

Brad Weber is a partner at Locke Lord and serves as the co-leader of the firm’s Antitrust Practice Group and AI Industry Group. Brad recently spoke with George Niño, the executive vice president for legal and compliance at Yokogawa Corporation of America.

Brad Weber: George, thank you for sharing your insights into effective corporate policies on the proper use of AI tools. First, can you tell us a little bit about your background and Yokogawa’s business?

George Niño: I grew up in a small town outside of Houston and always knew I wanted to be a lawyer. I developed an interest in international law issues, and shortly after law school I joined the Treasury Department in Washington, D.C. I worked as an international law enforcement specialist negotiating anti-money laundering banking treaties with other countries. I later worked for the Justice Department prosecuting gun and drug cases before returning to Houston to begin a career as a Texas trial attorney.

In 2018, I became the general counsel of both Yokogawa Corporation of America and KBC Advanced Technologies. The ultimate parent company of YCA and KBC is Yokogawa Electric Corporation, a company publicly traded on the Tokyo Stock Exchange that operates in 60 countries..

Yokogawa provides advanced solutions in the areas of measurement, control, and information to customers across a broad range of industries, including energy, chemicals, materials, pharmaceuticals, and food. Yokogawa addresses customer issues regarding the optimization of production, assets, and the supply chain with the effective application of digital technologies, enabling the transition to autonomous operations.

I joined the Yokogawa family because of its stellar reputation as a leading innovator in industrial automation and because I had the opportunity to work again on international legal issues with colleagues across the globe, including Japan, the European Union and the Middle East. My areas of responsibility for YCA and KBC include contract negotiations, mergers and acquisitions, compliance, business ethics, corporate governance, dispute resolutions and intellectual property.

Weber: ***I understand that Yokogawa recently adopted a corporate policy on the use of AI tools. Can you tell us how that came about?***

Niño: Sure. In November 2022, OpenAI publicly released ChatGPT based on a version of GPT-3.5. My children and their friends immediately adopted it as a tool for school and work. It is estimated that ChatGPT hit 100 million monthly active users in record time — just a couple of months after its release.

I did not spend much time with ChatGPT until March 2023 when OpenAI released ChatGPT Plus (or ChatGPT-4) based on GPT-4. This powerful new version of ChatGPT received a lot of attention from the media and businesses as people explored its speed, accuracy and the ability to incorporate its use into everyday life and work.

OpenAI describes GPT-4 as being 10 times more advanced than GPT-3.5. In addition, GPT-4 is multimodal, which means it can comprehend different information formats like photographs or other visuals. One commentator described ChatGPT-4 as developing "eyes." As one measure of its power, in March, GPT-4 scored in the 90th percentile on the Uniform Bar Exam, which was much higher than GPT-3.5's score only a few months earlier.

Initially, I focused on the upside of ChatGPT and how Yokogawa could incorporate it into our business workflows. I also thought that at least some people in our company might already be using it despite the fact that we did not have a usage policy, and I needed to consider the risks.

Then I started reading about significant data breaches in which employees at companies, including multinational, sophisticated companies, loaded source code and other confidential, internal company data into ChatGPT. Under OpenAI's terms of use at the time, those employee chats or conversations resulted in confidential company information being uploaded into OpenAI's database to train the model. This means that those companies lost control of some of their most sensitive data because of employees' improper use of ChatGPT.

I soon developed a new sense of urgency around the risks related to the use of ChatGPT. The actions that ChatGPT did well, like debugging or writing code and summarizing volumes of text and data, meant that employees would be drawn to it and possibly upload some of their employer's most confidential data. Though many employees received training on the proper handling of confidential information, at least some of them seemed to view ChatGPT differently and willingly uploaded highly-sensitive information into the application.

To address this risk, I knew I needed to draft an AI tools usage policy and roll it out as soon as possible.

Weber: ***What are some of the things you considered when deciding what to include in Yokogawa's AI policy?***

Niño: In March, I wanted to learn from the work of others in this area, so I researched how other companies responded to ChatGPT. I also asked other attorneys how their law firms and companies advised their employees on the use of ChatGPT. I then started using ChatGPT often to become familiar with it.

I quickly learned that companies at that time seemed to fall into one of two extreme camps. Some companies were so concerned about ChatGPT and possible data breaches that they banned its use outright. Other companies were not concerned at all about ChatGPT and thought their general confidentiality policies were sufficient guidance for their employees, so they did not see the need for a separate AI tools (ChatGPT) usage policy.

I determined that these two camps could not both be correct. I also soon came to realize that if you issued a total ban on the use of ChatGPT, some employees, like software engineers, might consider it to be so critical to their work that they would disregard the ban. I also thought that, given the frequent news about additional data breaches, people clearly were misusing ChatGPT and needed some guidance.

Ultimately, I concluded that the best option should be a policy somewhere in the middle of these two extremes. The policy should list clear and concise restrictions on certain uses of ChatGPT, but also describe other permitted uses of the tool with an explanation of why this was necessary. Since many other competitors of OpenAI were rolling out their own versions of generative AI products — such as Claude, Bard, Perplexity and others — I decided to call this an AI tools usage policy and not just a ChatGPT policy.

To determine what to include in the policy, I read as much as I could about these AI tools, including law review articles and technical articles describing the risks and benefits. I also started posting about this topic on LinkedIn in an effort to interact with others who were thinking about this issue and to share the knowledge I had gathered through my research.

In April, I decided to use ChatGPT to assist me in drafting a policy, and I posted about my experience on LinkedIn. My post asked: "Who else is thinking about asking ChatGPT to help draft a corporate policy for employees regarding the proper use of ChatGPT?" This question seemed to strike a chord, as it became my single most popular LinkedIn post (almost 11,000 impressions), and attorneys started contacting me to ask what to include in their own policies.

Weber: ***Is there anything in Yokogawa's AI policy that wasn't even a real consideration when you started the process of drafting the policy?***

Niño: Yes, initially OpenAI did not provide the option for a user to turn off ChatGPT's chat history. In April, OpenAI announced that it would allow users to turn off chat history and, when users select this option, their conversations will not be used to train and improve OpenAI's models. When chat history is disabled, OpenAI still will retain new conversations for 30 days, review them only when needed to monitor for abuse and then permanently delete them. This addressed some of the data privacy concerns

I had regarding the uploading of sensitive company information into OpenAI's database when our employees used ChatGPT.

Once I learned about this optional setting, I added a requirement in the policy that employees must enable it when using ChatGPT. I also alerted my LinkedIn network about this ChatGPT setting and described the steps to enable it so other general counsels I knew could consider notifying their employees.

Weber: ***For companies deciding whether to adopt a corporate AI policy, what are some important issues they should be considering?***

Niño: If employees believe an AI tool can help them complete their projects faster and better, there will be a strong temptation to use the AI tool. Because of this, I think it is fair to say that even if a company bans the use of AI tools on company devices, such as laptop computers, some employees will continue to use the tools on their own personal devices. As a result, companies should assume that at least some of their employees will use AI tools and should make awareness a policy and training a priority before data breaches occur.

Unless a company's business is highly regulated or has special concerns, I think a clear and concise policy is best.

First, the policy should prohibit certain types of uses — such as uploading confidential company data, business partner data or personal information — and only permit the use of AI tools in compliance with applicable laws and regulations.

Second, it should list certain permitted uses of AI tools, all of which are subject to the policy's general restrictions. For example, subject to the restrictions, a company could permit the use of AI tools for certain types of market research or to create or summarize certain documents based on publicly-available information.

Third, since these AI tools are prone to occasional hallucinations, inaccuracies and biased outputs, the policy should require a person to review all content created by the tools for accuracy and appropriateness before publicizing or disseminating the content.

Most importantly, all employees should be instructed to enable the data privacy settings on the tools they use, which in the case of ChatGPT means turning off the chat history.

Weber: ***Do you have any other observations about corporate AI policies you care to share?***

Niño: This is a rapidly developing area with AI tools being used in new and different ways through, for example, new plugins and products. It may seem obvious, but each of these new uses involve risk, and attorneys need to be agile and ready to react to and minimize these risks. Current hot topics in this area concern issues like confidentiality, data protection and privacy, cybersecurity, creation and protection of intellectual property and litigation.

In the same way that parties in litigation request electronically stored information during discovery, you could expect a party in a legal dispute to demand the ChatGPT chat history relevant to the issues in the case. Similarly, a recent article disclosed that over 100,000 compromised ChatGPT accounts are available for sale on the Dark Web. If those account holders had not disabled their chat history, then their chats, including any sensitive company information they posted in their chats, would be available to the hackers and buyers of these stolen credentials. Both are examples of why companies should instruct their employees to disable chat history on ChatGPT.

Another issue to consider is requiring your company's business partners, suppliers and vendors with whom you share confidential information to confirm that they have an effective AI tools policy that is enforced and followed by their employees. This is similar to corporate policies requiring a supplier to acknowledge its compliance with a supplier code of conduct, including guidance on issues like forced labor.

Given all of the reported and unreported data breaches, the more awareness and training that companies can provide to their employees on these AI issues the better.

Finally, for attorneys, I would encourage you to read about these AI tools, work with them often and become comfortable using them. They are the future, and the future is here. As one commentator said, AI likely will not take your job, but someone who knows how to use AI tools might.

Brad Weber *is the co-chair of Locke Lord's Antitrust Practice Group and Artificial Intelligence Industry Group, working in both the Dallas and Washington, D.C., offices. He also is a past chair of the Antitrust & Business Litigation Section of the State Bar of Texas, a former director on the board of the State Bar of Texas, a past president of the Dallas Bar Association and a past chair of the Dallas Bar Foundation.*

George Niño is general counsel and corporate secretary for two Yokogawa companies, Yokogawa Corporation of America and KBC Advanced Technologies.