Westlaw Today
powered by Reuters

3 natural guardrails for the safe use of generative AI

By Michael K. Atkinson, Esq., and Jacob Canter, Esq., Crowell & Moring LLP

JULY 13, 2023

Generative artificial intelligence ("GAI") is powerful technology that can unlock significant productivity improvements to help your business grow. But it can also be misused,[1] and even well-meaning uses can be harmful.[2]

Recently, we have found that if you run a business, the question has shifted from "should my company use GAI" to "how can we safely use GAI." Simply staying out of the game is still an option, but it may now be the riskiest — you will either fall behind, or your employees will use the tools without any guidance.

> *GAI is valuable when it simplifies and streamlines your business by completing tasks that can benefit from automation. But it is not a replacement for human judgment.*

Whether a Fortune 200 company or an energetic startup, we recommend first adopting these three principles whenever implementing or using GAI:

***First*, do not input any information or data that you are not OK disclosing.** The technology is not so different than how much software operates: (1) you input information; (2) that information is analyzed by someone else's technology; and (3) based on the third-party analysis a response is output. But once your information is input into someone else's system, it is not private anymore.

The disclosure of sensitive information[3] can harm your business and risk liability. If you allow or accidentally input another's intellectual property into a GAI system, you may be directly or indirectly at risk of copyright infringement. For example, OpenAI was recently served a class action complaint[4] alleging that ChatGPT improperly misuses and infringes copyrighted material to train the technology.

***Second*, always double-check your work.** The ChatGPT output can look and sound confident. That is no replacement for actually confirming whether the answer is correct. All the technology does is generate a relevant response based on test data. A response, however, can be relevant based on test data that is also false. And a response can be relevant based on test data that reinforces or exacerbates bias.

GAI is valuable when it simplifies and streamlines your business by completing tasks that can benefit from automation. But it is not a replacement for human judgment. For example, in Federal Court in New York City two lawyers were fined[5] for submitting a brief with citations that ChatGPT fabricated. Lawyers, the Judge explained, have a duty to ensure their filings are accurate. Customers and clients expect and demand accurate results as well.

***Third*, ask lots of questions.** Before you license GAI, determine how the vendor uses the data you input into their system. Determine whether the vendor is using the data to train its technology and whether it is disclosing that data to third parties.

Ask also what cybersecurity safeguards are present and whether it has a team that handles data privacy and protection. And ask what sub-vendors the vendor relies on to operate its software, what those sub-vendors do with the data they collect, and how those sub-vendors protect that data.

> *Before you license GAI, determine how the vendor uses the data you input into their system.*

To be sure, the conversation should not end here. Your company may need to draft new internal policies for GAI use or may need to update existing licenses.

Your company may also need to create educational materials, hold training sessions, set up technical protocols, enhance monitoring controls, or establish an audit system for the safe use of GAI systems. Your company may even decide, as some already have, to stand up your own customized GAI models or, alternatively, to forbid the use of GAI entirely until more information about the technology is known and better business practices are set.

Regardless of your company's specific approach to using GAI, you may also want to engage in the public discussion about GAI governance that is currently taking place in the United States and abroad. There have already been several U.S. Senate subcommittee hearings on GAI and how it will impact topics as diverse as commerce,[6] intellectual property,[7] and human rights.[8]

The European Union is closing in on passing an omnibus law governing the use of artificial intelligence in its jurisdiction (the "EU AI Act").[9] Federal and state lawmakers have made public statements about the promises and perils of the technology, sometimes also hinting at legislation.[10] Industry and civil society leaders have signed a joint statement[11] on global priorities that should be taken to mitigate the potential risks that GAI could cause.

The public discussion about GAI has the potential to help shape how this new technology is governed for years to come. For this reason alone, it is worthwhile to monitor. But there are also ways to be more directly involved in the discussion.

You can consider attending DEF CON, the longest running and largest computer security and hacking conference in the U.S., and go to the new AI Village[12] at this conference. Or if you are more technically savvy, consider participating in the National Institute for Standards and Technology's (NIST) public working group on generative artificial intelligence.[13] Even just setting up a small *ad hoc* committee at your company to think strategically about how GAI can improve your business is a worthwhile endeavor.

Every business leader will need to answer these questions of how to safely and effectively use GAI. Just as it is a mistake to trust GAI without question, it is a mistake to act like the questions around GAI can be ignored. GAI is here to stay and the time to act is now.

Notes

[1] https://bit.ly/3XMXv6w

[2] https://bit.ly/3roNUac

[3] https://bit.ly/3D5kzE3

[4] https://bit.ly/3D9U28R

[5] https://bit.ly/3JSN6ki

[6] https://bit.ly/44B6c6q

[7] https://bit.ly/3rqei3c

[8] https://bit.ly/44lKJyG

[9] https://bit.ly/44xUObX

[10] https://bit.ly/3XKjwD3

[11] https://bit.ly/3O6LOEx

[12] https://bit.ly/46JjSy8

[13] https://bit.ly/3pE6GtF

About the authors

Michael K. Atkinson (L) is a partner with **Crowell & Moring LLP** in the firm's Washington, D.C. office. He is also a professorial lecturer in law on artificial intelligence law & policy at The George Washington University Law School and a former inspector general of the U.S. Intelligence Community. He can be reached at matkinson@crowell.com. **Jacob Canter** (R) is an associate who joined the firm's San Francisco office after clerking in the Southern District of New York. His practices focuses on litigation, technology, privacy and cybersecurity. He can be reached at jcanter@crowell.com.

This article was first published on Westlaw Today on July 13, 2023.