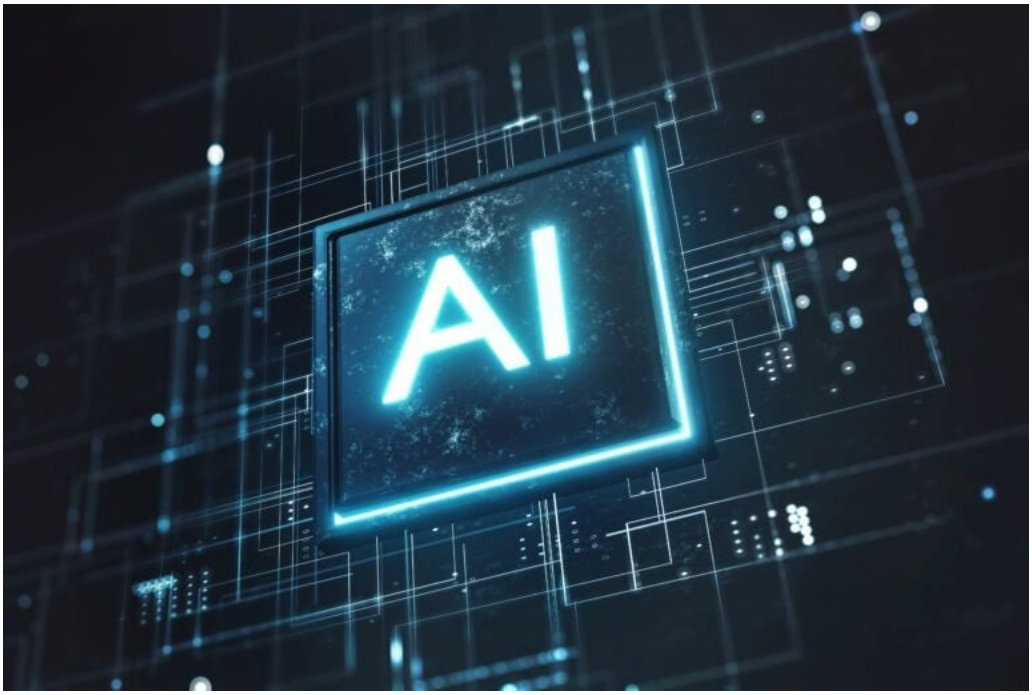
Innovation and Accountability: Asking Better Questions in Implementing Generative AI

Cynthia Cole, et al.

Cybersecurity Law Report (2023)

Innovation and Accountability: Asking Better Questions in Implementing Generative AI

AUGUST 10, 2023 by CYNTHIA COLE, RACHEL EHLERS AND BRYCE BAILEY 12 MINS READ



There has been an incredible volume of discussion around generative AI (GAI) in 2023, including products like ChatGPT and GitHub Copilot, and the potential impact these tools have on every corner of the business world. This is not surprising given that GAI has demonstrated powerful functionality, making it easy to hypothesize about use cases.

Unfortunately, on top of the fervor, the use of GAI presents a multitude of risks. Some companies have banned GAI use outright, at least for the short term, because of potential trouble, which includes insufficient security, inaccurate outputs and intellectual property (IP) issues ranging from IP loss to potential infringement, with several copyright claims filed and starting their way through

the courts. Other concerns include use of personal information and what data sets are used in AI training models.

Companies that are banning the use of GAI are losing the benefits that these tools can provide. Many companies already rely heavily on AI, thus an outright ban on GAI may not be practical. As companies attempt to understand how AI already exists in their business, and at the same time expand its use, they should consider a larger set of risk factors than they have to date. This article focuses on some of the most important issues that companies should explore as they try to understand GAI and consider incorporating it into their business.

Why is Large-Scale GAI Adoption Risky?

GAI can carry a host of IP and other risks, including:

- loss of trade secrets or other company proprietary information;
- potential infringement of existing third-party IP;
- potential violation of data privacy regulations and individual data rights; and
- risk of violating other companies' terms and conditions.

To fully understand the risks, it is helpful to better understand how GAI works.

GAI leverages machine learning technology to (i) collect large amounts of data, (ii) analyze that data, and then (iii) predictively generate an output based on the input request and the relevant data that was analyzed. At the heart of the tool is a neural network-based system that uses algorithms to spot patterns within the data and make predictions. A central part of GAI development is training and retraining algorithms that run the neural network.

A key concern with AI is that users have little insight into *how* an AI makes decisions. There is minimal visibility into the way an AI tool takes in data, reviews and learns from the data, and then provides the requested content. *What* it creates can be seen, but an explanation of *how* it was created is not always available.
GAI tools need a large amount of data to function well and, if left unrestricted, users may have limited insight into what internal and proprietary information

they may access for outputs. Additionally, whenever data is fed into the AI directly, this data likely will be leveraged by the tool for future outputs.

Trade Secret Disclosure

To the extent that an employee, or anyone else, puts proprietary information into a GAI bot, or a bot has access to internal systems that contain such information, there is a risk of losing trade secret protection on that information. In the U.S. and many other jurisdictions, companies are required to make reasonable efforts to maintain trade secret protection. A company that does not have proper safeguards around GAI and does not ensure that contractors or vendors with access to its data use safeguards, arguably is not making reasonable efforts to protect its information and reduce the risk of trade secret disclosure.

This disclosure issue, including the possible loss of proprietary source code, has already been observed at major companies. Many companies struggle with the need to implement and maintain processes and procedures around IP development, while moving quickly to create innovative IP in a competitive market. If employees do not have proper guidance around the tools they are able to use in development, then there can be a disclosure issue, *e.g.*, an employee using an AI tool that is not designed for confidential work product or inputs. Employers should be checking in with their development and product teams to properly vet the tools they are using and bolster any policies currently in place – or create new ones – to address the increased desire for, and ease of use of, AI tools.

IP Infringement

Additionally, a company may not know what *other* company's IP was used to train an AI bot that it leverages. GAI tools do not discriminate against information subject to copyright, trademark or patent protection. And because of the black-box structure, it may be difficult to know if outputs may be relying on protected information, thereby subjecting the company to the risk of infringement claims.

In April 2023, an online content creator was praised (and criticized) for music developed through GAI. The creator was able to simulate the sound and vocal stylings of a song by the hip-hop artist Drake. The tool presumably leveraged Drake's own music, which was copyrighted. It is too early to determine how this infringement will be addressed by a court.

Data Privacy Risks

Data privacy risks are similar: users do not know what personal information a GAI bot may collect during their chat sessions. Additionally, when companies use these tools, they likely do not know whether and how that personal information is being processed or, conversely, the source of the personal information being produced by the tool. If the tool and anything built with it is found to be violating individual rights around personal information, then the business may have to remove the tool and delete its results. If the tool is part of another commercialized product or service, then the company will have to ask its customers to do the same.

Terms and Conditions Abound

Almost all websites are governed by a set of terms and conditions for access and use, many of which forbid data scraping of even the publicly available information found on them. Though subject to certain obligations, data scraping is not illegal in most jurisdictions unless it violates a website's terms and conditions or is a violation of someone's individual or property rights, like copyright. Thus, any information taken from those websites is subject to the stated obligations and protections, especially if the information is eventually leveraged for commercial use.

Using GAI, which may have pulled information from websites through data scraping, may expose the user to a significant number of additional obligations. If the AI tool is found to have violated the terms and conditions of third-party websites, then the tool may have collected data unlawfully. As is the case with unlawful use of personal information, the ultimate users of the tool may then be subject to disgorgement or other potential violations. If the source of data in the AI tool is not properly vetted, those unlawful collection issues could pass through to the user.

How Companies Can Protect Themselves

Fortunately, there are protections and restrictions companies can implement around the use of GAI. These restrictions and protections can be used both internally and in agreements with third parties that may be leveraging GAI.

Involve Cross-Functional Teams and Leadership

Because AI-enabled functions are increasingly incorporated into applications across the enterprise technology stack, GAI-related issues are arising in all types of business transactions. Companies should develop cross-functional teams that include legal, procurement, IT, HR, marketing, product, information security, compliance, data analytics and risk functions, among others, to review and address use cases and concerns.

Companies should also include executive leadership in AI discussions to help set company policies, educate employees on the risks and opportunities with these novel technologies, and provide support in navigating the emerging GAI landscape. The misuse of AI tools, or the correct use of the wrong one, involves significant risk for a company – from bad press to protracted legal action.

Executive leadership should set the tone and create alignment within the organization that will help bring focus to the cross-functional teams tasked with evaluation of AI use.

Learn About the Specific AI Tools

Whether using the GAI application internally or contracting with a third party that leverages a GAI tool, companies should review the tool to learn:

- how the GAI tool is trained, and what data it relies on for training;
- if there are any limitations on what data it can use for training;
- how the GAI stores and processes data; and
- what security measures are built into the GAI tool.

Organizations should build these considerations into their existing procurement processes with standardized questionnaires, whether that means having a stand-alone set of questions or incorporating them into larger, more general questionnaires. Information sheets provided by third-party AI tools should be reviewed by cross-functional teams and, where possible, vetted for accuracy with further questions, and even benchmarking against competitor claims.

Obtaining information from vendors can be difficult, as many developers consider such details to be commercially sensitive. In practice, vendors also may

not have complete information about how the AI models in their products have been trained.

If possible, do informal benchmarking by asking to talk to other users to see if they are happy with the tools' results. Above all, do not be afraid to ask probative questions and to request contractual protections like expanded liability and indemnification.

In response to some of the recent negative press about the risk of GAI, many AI tool providers are now expanding their standard indemnification obligations to users to show that they stand behind their tools and, most importantly, that they stand behind the integrity of the data in their data sets.

Be Specific About the Intended Use

It is critical to have a clear understanding of how and where a GAI tool will be used, including:

- Who are the intended users?
- What sensitive information do those users have access to?
- When should the tool be used?
- What alternative tools could be used?
- What other programs or tools may be integrated with the AI tool?
- What information do *those* tools have access to?

As suggested above, companies should have cross-functional teams in place to review these questions. Companies' procurement and legal teams should read the statement of work and deliverables very carefully to ensure that they align with their stated intended use, whether internal or external.

Consider the Rights and Obligations Implicated

Consider all the relevant rights and obligations at play when drafting vendor contracts where a GAI tool will be used, and address assigning ownership, risks and indemnification. The following should be reviewed:

- Who owns content developed and derived from the AI tool?
- Is one party indemnifying the other for violations or infringements caused by the AI tool?
- Who is responsible for ensuring that the AI tool complies with applicable laws?
- Can liability arising from such risks be allocated effectively with standard contractual representations and warranties, or is a bespoke approach required, particularly to address issues around transparency and fairness that arise in the AI context?
- What data privacy regulations may be triggered by the AI tool?
- Does the AI tool rely on any proprietary information? If so, how will the security of that information be maintained?

Companies should also consider what steps are being taken to protect the rights and enforce the obligations of these agreements. For example, consider what protections and requirements each side should put in place, what internal policies should govern the AI use, and what requirements clients or third parties have in place around the use of AI.

GAI abounds with promise in many ways, but the perfect risk storm created around its use is only just now being felt. In addition to the more practical matters, reliance on automated tools causes issues of transparency and bias in decision making. While it is difficult to contractually assign responsibility for bias in results, one way that users protect themselves is by having flexible termination provisions in agreements with AI vendors where the desired results are not achieved or are inherently flawed.

No matter the promise of innovation, ultimately the only way to measure and allocate results and responsibility in GAI is through human oversight and accountability – asking better questions and auditing results.

Cynthia Cole is an IP partner in Baker McKenzie's Palo Alto office. She advises clients across a wide range of industries including technology; media and telecoms; energy; mining and infrastructure; healthcare and life sciences; and industrials, manufacturing and transportation. Cole has extensive experience in complex technology and intellectual property alliances and transactions. Her practice also includes providing intellectual property and data privacy and security assistance in

connection with M&A, private equity and other corporate transactions. Cole previously has served in-house as CEO and general counsel, and currently acts as outside general counsel to a number of executive teams and boards of directors.

Rachel Ehlers is a partner in Baker McKenzie's intellectual property and technology practice group, based in the firm's Houston office. With a focus on technology transactions, data privacy and cybersecurity, she advises clients on data incidents and breach response, cross-border transfers, and data privacy and cybersecurity issues related to mergers and acquisitions. Earlier in her career, Ehlers served in multiple in-house legal and compliance roles, and has provided guidance and training to multinational companies globally.

Bryce Bailey is an associate in Baker McKenzie's IP practice group. His experience includes patent prosecution, IP litigation and technology transactions. As part of the firm's North American trade secrets practice, Bailey assists the technology transactions attorneys with the assessment of IP and data privacy details.