Proskauer

ChatGPT Risks and the Need for Corporate Policies

New Media and Technology Law Blog on **February 23, 2022**

ChatGPT has quickly become the talk of business, media and the Internet – reportedly, there were over 100 million monthly active users of the application just in January alone.

While there are many stories of the creative, humorous, apologetic, and in some cases unsettling interactions with ChatGPT,[1] the potential business applications for ChatGPT and other emerging generative artificial intelligence applications (generally referred to in this post as "GAI") are plentiful. Many businesses see GAI as a potential game-changer. But, like other new foundational technology developments, new issues and possible areas of risk are presented.

ChatGPT is being used by employees and consultants in business today. Thus, businesses are well advised to evaluate the issues and risks to determine what policies or technical guardrails, if any, should be imposed on GAI's use in the workplace.

What are the risks?

Confidentiality. While it may be tempting to use GAI to further develop or refine business strategies, software or other proprietary information, the input of confidential information into ChatGPT and other GAIs presents a number of risks:

- ChatGPT may train on the input that is provided,[2] and thus it is possible that portions of that inputted confidential information may be provided, in some form, to a subsequent user. Indeed, it was reported that at least one company advised employees not to input confidential code into the application for data security concerns.[3]
- Some confidential business information may be licensed from third parties and may be subject to confidentiality requirements or restrictions on use, and by putting such information into ChatGPT, a company may be in violation of those restrictions.
- Trade secret law requires one to maintain reasonable steps to protect the secrecy of information claimed to be a trade secret, and putting information into ChatGPT may weaken a company's position that such information is actually, as a matter of law, protectable as a trade secret.

- Privacy laws may restrict the submission of personal information of employees, clients, affiliates or consumers into any GAI.

Regulatory Issues.

To the extent a regulated business is using ChatGPT or other GAI in its business operations, thought should be given to whether some or all of that use is subject to regulatory requirements. For example, should or must some of the interactions be logged, recorded, archived in some manner? The analysis of this issue will possibly be informed by applicable law, contract, insurance-based requirements, as well as possibly a company's own internal policies.

Intellectual Property. GAI presents a number of interesting and new intellectual property issues:

- Does training of GAI via scraping the web constitute an intellectual property infringement or DMCA violation for the removal of CMI (copyright management information), and if so, can the user of that GAI be found to be liable in any way?
- What is the IP status of the output of GAI? For example, if a software developer uses ChatGPT to create software, can that developer represent to its user that the developer owns all IP rights in that software? Can the developer indemnify the user for infringement issues? And what is the status of GAI-generated images, which often bear a recognizable similarity to one or more of their human-created sources?
- To the extent the use of GAI is infringing, is the fair use or implied license doctrine relevant?
- Can a GAI or the user of GAI be an "inventor" under patent law or an owner of a U.S. copyright in GAI-generated material?

These intellectual property issues are, to varying degrees, all open questions, with litigants just beginning to bring suit and ask some of these questions. However, a few basic principles are clear:

- It is best practice to avoid claiming copyright in GAI-generated content (particularly in AI-generated artwork or images). ChatGPT's terms are instructive. The terms cover rights in content: "As between the parties and to the extent permitted by applicable law, you own all Input, and subject to your compliance with these Terms, OpenAI hereby assigns to you all its right, title and interest in and to Output." While such license to the output is a broad grant of OpenAI's rights in the Output, it is not definitive that ChatGPT has any rights in the Output to grant at all.

- Consideration should be given as to whether third party software developers or content creators of any kind should be permitted to use ChatGPT or any GAI in their deliverables. This is an issue that should be addressed in development agreements with those third parties.
- Copyright Office policy, as currently stated in the *Compendium of U.S. Copyright Office Practices* (3d Ed. 2021), is that the Copyright Office "will not register works produced by a machine or mere mechanical process that operates randomly or automatically without any creative input or intervention from a human author. The crucial question is 'whether the 'work' is basically one of human authorship, with the computer [or other device] merely being an assisting instrument, or whether the traditional elements of authorship in the work...were actually conceived and executed not by man but by a machine.'" (See also *Trade-Mark Cases*, 100 U.S. 82, 94 (1879) (copyright law only protects "the fruits of intellectual labor" that "are founded in the creative powers of the mind"). Thus, based on this policy, GAI-generated content would not be subject to copyright protection.

Quality and Output Issues.

There are a number of issues that are presented by the nature of GAI's output:

- ChatGPT and the other GAIs are still works-in-progress with limitations. As OpenAI has advised: "ChatGPT sometimes writes plausible-sounding but incorrect or nonsensical answers." Thus, while the current ChatGPT interface is ready to use "out of the box," the accuracy and truth of any output must be confirmed before finalizing or publishing any work product.
- GAI-generated analysis may reflect biased or discriminatory content on which it was trained.[4] Along with fact-checking the veracity of ChatGPT and other GAI output, users should be attuned to any discriminatory or biased statements or conclusions resulting in the algorithmic mining of such source materials. This could be a particular concern in the context of employment discrimination laws and laws regulating the use of artificial intelligence in employment decisions.
- Publishers and other content creators often procure "Errors and Omissions" insurance to cover exposure based on infringement and other risks. Often the underwriting of those policies involves a review of internal content creation practices. Will GAI-generated content be within the scope of traditional errors and omissions policies?
- Section 230 of the Communications Decency Act is highly controversial in its scope and application. To the extent GAI-generated content is used in an online business, it is unclear if and to what extent the CDA would apply with respect to that content. CDA § 230 prohibits a "provider or user of an interactive computer service" from

being held responsible "as the publisher or speaker of any information provided by another information content provider." Are there any situations where GAI-generated content would not be considered "information provided by another information provider"? These types of third-party content issues are especially fraught, as the Supreme Court just heard argument on February 21, 2023 in a case examining the applicability of the CDA to algorithmic functions.

- Thought should be given to whether GAI-generated content should be identified as such when made public. This may be an issue if the content is generated in a real-time fashion, e.g., in a bot conversation with a customer or employee. Organizations should also consider whether such disclosures are appropriate to clients, business partners or the public.
- Are GAI interactions discoverable in litigation? Should a company's document retention policy specifically address GAI-generated content?

Artificial Intelligence Compliance Issues

There are a number of laws and regulations place and in various stages of enactment in the United States and abroad that address the use of artificial intelligence. For example, California's chatbot law (Bus. and Prof. Code § 17940) requires, among other things, that in certain consumer interactions, a company provide clear and conspicuous disclosure that the consumer is interacting with a bot. Moreover, New York City and several states have regulations impacting automated decision-making in the employment context and the FTC and state attorneys general have enforcement powers against "unfair or deceptive" trade practices. Organizations must ensure that their use of GAI is compliant with such laws.

Thoughts on Policies

ChatGPT is being used today. Organizations cannot ignore it and the inevitability of the even wider use of these technologies in the near future. Every organization should be evaluating the issues GAI presents to determine to what degree they present material risk to the organization. Each entity must approach GAI from its own particular risk profile. Indeed, as outlined in the National Institute of Standards and Technology's (NIST) recently published *Artificial Intelligence Risk Management Framework 1.0,* risk tolerances can change over time as AI systems, policies, and norms evolve.[5]

Possible courses of action include the following:

- Messaging to the relevant community that the use of GAI is permitted, but outlining the power and risks of GAI and asking the community to be vigilant.
- Enacting policies that may do some or all of the following:
- Precluding certain uses of GAI. News reports suggest that some companies have already taken actions to restrict employee use of ChatGPT.
- Identifying permitted uses of GAI, and the cases in which prior approval is required
- Requiring internal tracking of the use of GAI and additional human review of selected GAI-generated content
- Addressing external disclosures of the use of GAI and GAI output
- Regulating the uses of GAI by external business partners and vendors.
- Addressing the possibility of embedding GAI applications on the company's website

We are likely just at the start of a cycle of innovation surrounding generative AI technology and its application for businesses and consumers, much like the early days of e-commerce or web 2.0 or the current days of web 3.0. Of course this post highlights just some of the preliminary issues and concerns associated with GAI — there will likely be many more issues to unpack in the future as the technology evolves. To the extent an organization perceives GAI to present any of the risks highlighted above, or views GAI to present other issues for its business, putting appropriate policies in place now may be helpful.

---

[1] A Feb. 16, 2023 post on the OpenAI Blog noted that the company has received copies of biased or offensive outputs from users, noting that in many cases the responses showed limitations of the system that will be addressed: "Many are rightly worried about biases in the design and impact of AI systems. We are committed to robustly addressing this issue and being transparent about both our intentions and our progress."

[2] As per the ChatGPT terms: "To help OpenAI provide and maintain the Services, you agree and instruct that we may use Content to develop and improve the Services."

[3] Organizations that are using ChatGPT's API and are concerned with such issues might consider using ChatGPT's opt-out procedure (outlined here).

[4] See generally: The White House, "Blueprint for an AI Bill of Rights" ("Algorithmic discrimination occurs when automated systems contribute to unjustified different treatment or impacts disfavoring people based on their race, color, ethnicity, sex…, religion, age, national origin, disability, veteran status, genetic information, or any other classification protected by law. Depending on the specific circumstances, such algorithmic discrimination may violate legal protections").

[5] The NIST framework recommends that organizations develop enhanced processes for governing, mapping, measuring, and managing AI risk and clearly define the roles and responsibilities for the personnel overseeing AI system usage and performance.

View original.

Related Professionals

- **Jeffrey D. Neuburger**