

Microsoft wants AI to change your job—if it can work out the kinks

November 2 2022, by Dina Bass



Credit: Pixabay/CC0 Public Domain

The most hyped words in tech today may be "generative AI." The term describes artificially intelligent technology that can generate art, or text or code, directed by prompts from a user. The concept was made famous this year by Dall-E, a program capable of creating a fantastic range of artistic images on command. Now a new program from Microsoft Corp.,

GitHub Copilot, seeks to transform the technology from internet sensation into something broadly useful.

Earlier this year, Microsoft-owned GitHub widely released the artificial intelligence tool to work alongside computer programmers. As they type, Copilot suggests snippets of code that could come next in the program, like an autocomplete bot trained to speak in the Python or JavaScript. It's particularly useful for the programming equivalent of manual labor—filling in chunks of code that are necessary, but not particularly complicated or creative.

The tool is currently in use by hundreds of thousands [software developers](#) who rely on it to generate up to 40% of the code they write in about a dozen of the most popular languages. GitHub believes that developers could use Copilot to write as much as 80% of their code within five years. That's just the beginning of the companies' ambition.

Microsoft executives told Bloomberg the company has plans to develop the Copilot technology for use in similar programs for other job categories, like office work, video-game design, architecture and computer security.

"We really do believe that GitHub Copilot is replicable to thousands of different types of knowledge work," said Microsoft Chief Technology Officer Kevin Scott. Microsoft will build some of these tools itself and others will come from partners, customers and rivals, Scott said.

Cassidy Williams, chief technology officer of AI startup Contenda, is a fan of GitHub Copilot and has been using it since its beta launch with increasing success. "I don't see it taking my job anytime soon," Williams said. "That being said, it has been particularly helpful for small things like helper functions, or even just getting me 80% of the way there."

But it also misfires, sometimes hilariously. Less than a year ago, when she asked it to name the most corrupt company, it answered Microsoft.

Williams' experience illustrates the promise and peril of generative AI. Besides offering coding help, its output can sometimes surprise or horrify. The category of AI tools used for Copilot are referred to as large language models, and they learn from human writing. The product is generally only as good as the data that goes into it—an issue that raises a thicket of novel ethical quandaries.

At times, AI can spit out hateful or racist speech. Software developers have complained that Copilot occasionally copies wholesale from their programs, raising concerns over ownership and copyright protections. And the program is capable of learning from insecure code, which means it has the potential to reproduce security flaws that let in hackers.

Microsoft is aware of the risks and conducted a safety review of the program prior to its release, Scott said. The company created a software layer that filters harmful content from its cloud AI services, and has tried to train these kind of programs to behave appropriately.

The price of failing here could be great. Sarah Bird, who leads responsible AI for Microsoft's Azure AI, the team that makes the ethics layer for Copilot, said these kinds of problems are make-or-break for the new class of products. "You can't really use these technologies in practice," she said, "if you don't also get the responsible AI part of the story right."

GitHub Copilot was created by GitHub in conjunction with OpenAI, a high-profile startup run by former Y Combinator president Sam Altman, and backed by investors including Microsoft.

The program shines when developers need to fill in simple coding—the

kinds of problems that they could solve by searching through GitHub's archive of opensource code. In a demonstration, Ryan Salva, vice president of product at GitHub, showed how a coder might select a programming language and start typing code that states they want a system for storing addresses. When they hit return, about a dozen lines of gray, italicized text appear. That's Copilot offering up a simple address book program.

The dream is to eliminate menial work. "What percent [of your time] is the mechanical stuff, versus the vision, and what do you want the vision to be?" said Greg Brockman, OpenAI's president and co-founder. "I want it to be at 90% and 10% implementation, but I can guarantee it's the opposite right now."

Eventually, the technology's uses will expand. For example, this kind of program could allow video-game makers to auto-create dialogue for non-player characters, Scott said. Conversations in games that often feel stilted or repetitive—from, say, villagers, soldiers and other background characters—could suddenly become engaging and responsive.

Microsoft's cybersecurity products team is also in the early stages of figuring out how AI can help fend off hackers, said Vasu Jakkal, a Microsoft security vice president.

As Microsoft develops additional uses for Copilot-like technology, it's also helping partners create their own programs using the Microsoft service Azure OpenAI. The company is already working with Autodesk on its Maya three-dimensional animation and modeling product, which could add assistive features for architects and industrial design, Chief Executive Officer Satya Nadella said at a conference in October.

Proponents of GitHub Copilot and programs like it believe that it could make coding accessible for non-experts. In addition to drawing from Azure OpenAI, Copilot relies on an OpenAI programming tool called

Codex. Codex lets programmers use plain language, rather than code, to speak what they want into existence. During a May keynote by Scott, a Microsoft engineer demonstrated how Codex could follow plain English commands to write code to make a Minecraft character walk, look, craft a torch and answer questions.

The company also thinks it could develop virtual assistants for Word and Excel, or one for Microsoft Teams to perform tasks like recording and summarizing conversations. The idea calls to mind Clippy, Microsoft's beloved but oft-maligned talking paperclip. The company will have to be careful not get carried away by the new technology or use it for "PR stunts," Scott said.

"We don't want to build a bunch of superfluous stuff that is there, and it sort of looks cute, and you use it once and then never again," Scott said. "We have built something that is genuinely very, very useful and not another Clippy."

Despite their utility, there are also risks that come with these kinds of AI programs. That's mostly because of the unruly data they take in. "One of the big problems with large language models is they're generally trained on data that is not well documented," said Margaret Mitchell, an AI ethics researcher and co-author of a seminal paper on the dangers of large language models. "Racism can come in and safety issues can come in."

Early on, researchers at OpenAI and elsewhere recognized the threats. When generating a long chunk of text, AI programs can meander or generate hateful text or angry rants, Microsoft's Bird said. The programs also mimic human behavior without the benefits of a person's understanding of ethics. For example, language models have learned that when people speak or write, they often back up their assertions with a quote, so the programs sometimes do the same—only they make up the

quote and who said it, Bird said.

Even in Copilot, which generates text in programming languages, offensive speech can creep in, she said. Microsoft created a content filter that it layered on top of Copilot and Azure OpenAI that checks for harmful content. It also added human moderators with programming skills to keep tabs.

A separate, potentially even more difficult problem is that Copilot has the potential to recreate and spread security flaws. The program is trained on vast troves of programming code, some of it with known security problems. Microsoft and GitHub are wrestling with the possibility that Copilot could spit out insecure code—and that a hacker could figure out a way to teach Copilot to place vulnerabilities in programs.

Alex Hanna, research director at the Distributed AI Research Institute, believes that such an attack may be even harder to mitigate than biased speech, which Microsoft already has some experience blocking. The issue could get more serious as Copilot grows. "If this becomes very common as a tool and it's being used kind of widely in production systems, that's a bit more of a worry," Hanna said.

But the biggest ethical questions that have materialized for Copilot so far revolve around copyright issues. Some developers have complained that code it suggests looks suspiciously like their own work. GitHub said the tool can, in very rare cases, produce copied code. The current version tries to filter and prevent suggestions that match existing code in GitHub's public repositories. However, there's still considerable angst in some programmer communities.

It's possible that researchers and developers are able to overcome all of these challenges, and that AI programs will enjoy mass adoption. That

will, of course, raise a new challenge: the impact on the human workforce. If AI tech gets good enough, it could replace human workers. But Microsoft's Scott believes the impacts will be positive—he sees parallels to the gains of the Industrial Revolution.

"The thing that is going to move really, really, really fast is assisting people and giving folks more leverage with their cognitive work," Scott said. The name Copilot was intentional, he said. "It's not about building a pilot, it's about real assistive technology to help people get past all of the tedium that they've got in their repetitive cognitive work and get to the things that are uniquely human."

Right now the technology is not accurate enough to replace anyone, but is good enough to produce anxiety about the future. While the Industrial Revolution paved the way for the modern economy, it also put a lot of people out of a job.

For workers, the first question is, "How can I use these tools to become more effective, as opposed to you know, 'Oh, my God, this is my job,'" said James Governor, co-founder of analyst firm RedMonk. "But there are going to be structural changes here. The technical transformations and information transformations are always associated with a lot of scary stuff."

2022 Bloomberg L.P.

Distributed by Tribune Content Agency, LLC.

Citation: Microsoft wants AI to change your job—if it can work out the kinks (2022, November 2) retrieved 9 April 2024 from

<https://techxplore.com/news/2022-11-microsoft-ai-jobif-kinks.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.