ChatGPT is an AI chatbot developed by San Francisco-based startup OpenAI. The chatbot uses an LLM based on GPT model architecture and generates content in response to prompts it has not been explicitly trained on. It can pass the bar exam, pass the CPA Exam, and land a job at Google as a Level 3 Coder. ChatGPT is the culmination of advancements from the original GPT to the current model, GPT-3.5, which powers ChatGPT (Figure 1).

Although appearing to be an overnight sensation, ChatGPT came to be through a series of incremental improvements over time that reveal how future innovations and enhancements to GPT may transpire in the future. To use ChatGPT or other GPT models effectively, we need to understand what they are actually doing underneath the hood.

Within days of launching, OpenAI’s chatbot, “ChatGPT,” went viral and quickly became a media fixture. Gaining notoriety and influence, ChatGPT has become the most successful example of the power of large language models (LLMs)—the platform acquired 100 million active users in 2 months, a feat Instagram took 2.5 years to achieve. Trained on a vast set of knowledge, and built on a Generative Pre-trained Transformer (GPT), OpenAI’s chatbot revolutionized the usability of GPT models. By dramatically improving the underlying model’s generalizability and making it accessible in an easy-to-use interface, OpenAI has sparked a seemingly limitless level of enthusiasm and excitement about artificial intelligence (AI). With the potential to address a vast array of downstream use cases, ChatGPT serves as an exemplar for future GPT implementations where the possibilities seem endless but may face unexpected challenges. As with any new technology, organizations will need the right skills, experience, and perspective to best realize the value of this kind of innovation. To inform such perspectives, we offer the following informational white paper to explain what this technology is and how organizations can use it.

ChatGPT was trained on billions of words collected across the internet, books, and Wikipedia, totaling roughly 499B tokens. lifearchitect.ai/chatgpt/


cnbc.com/2023/01/31/google-testing-chatgpt-like-chatbot-apprentice-bard-with-employees.html
Large Language Models

By understanding the probability distribution of a sequence of words, LLMs generate the most likely next word given some context such as a prompt. Essentially, they predict text sequentially. These probabilities will vary if people use different training datasets and model architectures. Thus, effective use of these models for downstream tasks such as summarization, question-answering, or translation requires the selection of the appropriate training dataset(s) and model(s).

OpenAI pre-trained ChatGPT on large corpora of textual data from books, Wikipedia, research articles, websites, and other written content, comprising 300 billion words—about 570 giga-bytes of data. OpenAI then finetuned the model to perform conversational tasks by enabling it to handle queries or prompts. While ChatGPT’s breadth and scale are impressive, it is only as knowledgeable as the data on which it was trained. For example, it cannot answer factual questions about anything occurring after 2021 (the training data is limited). For ChatGPT to answer any question, it must use the input text as a prompt to generate an output. Without any additional fine-tuning, ChatGPT answers user queries with generally correct and informative responses—a dramatic change from traditional chatbots that can only answer queries limited to a specific scope.

Advancements in LLMs

The key advancement to the latest GPT model involved using Reinforcement Learning from Human Feedback (RLHF) in a three-step process: (1) pretrain an LLM; (2) acquire data to create a reward model based on human scoring; and (3) finetune the model with human input. These layers of technological advancements, as depicted in Figure 2, ultimately led to an unprecedented level of engagement and use. Without any additional fine-tuning, ChatGPT answers user queries with generally correct and comprehensive answers—a dramatic change from traditional chatbots that can only answer queries limited to a specific scope.

Prompt Engineering

While anyone with an internet connection and email address can use ChatGPT immediately, skilled users who understand how the underlying model works will write better prompts to extract significantly more value from ChatGPT. This is because LLMs use a concept called “prompting” or “priming.” A subfield of research called “prompt engineering” studies how to guide and interface with ChatGPT and other generative models. This subfield is poised to improve both the quality of output and the quality of human interaction and will help guide users in getting the most from generative LLMs.

Using ChatGPT is as simple as going to chat.openai.com. Users can create a free account and immediately begin typing questions or requests into a box. With a click of a button, users can witness ChatGPT’s power in action. ChatGPT can generate ideas, develop business strategies, create recipes, provide gift suggestions, and write blog posts. It also can help create clear and concise documentation for code, find bugs in code, explain code errors, and even generate code itself.

At a high level, ChatGPT can help knowledgeable users create content at exponentially faster speeds. It can help produce outputs that users can directly integrate into codebases, databases, and various components of a system, making the LLMs significantly more useful. There are four principles for prompts that every user should consider:

- **Show and tell**—be very clear in your instructions.
- **Break work into smaller, discrete chunks.**
ChatGPT’s capabilities transcend industries. Technology companies will not be the only organizations using ChatGPT, as it can provide value to a wide range of fields such as software development, healthcare, government and policy, military operations, and law.

Potential Use Cases in the Government

While the government is not typically an early adopter of new technology, it has several use cases similar to industry for proactively assessing and evaluating the benefits of employing a ChatGPT-like technology. Most use cases that involve highly repetitive tasks or processing large quantities of information can benefit from ChatGPT, and the government, like any organization, can realize substantial value in automating or accelerating all or parts of these tasks. However, ChatGPT is best used as a tool to augment the completion of human tasks rather than replace human workers. Some potential use cases in the government include:

Benefits and Considerations

There are several tangible benefits to using ChatGPT and similar technology, but businesses need to understand its long-term implications. Even though OpenAI is clearly demonstrating the value of ChatGPT, it only recently made available ChatGPT and Whisper models via API as of March 1, 2023.

Several questions remain around how enterprises will effectively use ChatGPT and related models. Still, ChatGPT offers financial savings, time efficiency, quality, and creativity. Examples of these benefits include the following:

- **Defense and Security**: Produce Intelligence Summaries and other standardized reporting; assist with characterizing potential threats
- **Regulatory Compliance**: Summarize/synthesize precedent and procedures to produce policy and regulatory guidance or answer inquiries on applicable law
- **Data Analytics**: Obtain summary statistics, explanations of data, including answers, predictions, recommendations, and even help on specific data analysis tasks
- **Training and Education**: Provide training and education to employees, assist in onboarding, provide technical support, and answer questions about policies and procedures
- **Citizen Services**: Automate citizen services inquiries and support, including answering FAQs, providing personalized assistance, and directing inquiries to the appropriate departments or agencies

**Figure 4: Examples of Potential Government Use Cases**
Despite ChatGPT having clear benefits, there remain several unknowns about its use that all organizations should take into account:

- **Undefined Legal Rights:** Outstanding questions around ownership of data, model, intellectual property rights, and privacy persist.

- **AI Safety and Responsibility:** Measures to prevent intended and unintended harm—especially as they relate to AI Ethics and associated human, environmental, and societal effects—remain uncertain.

- **Bias:** Like all LLMs trained on internet corpora, ChatGPT captures and potentially perpetuates biases inherited from any part of its training datasets.

- **Accuracy:** ChatGPT may not always provide factually correct information and needs safeguards in place even for lower risk uses.

- **Cost:** Estimated at $100,000 a day to run, ChatGPT consumes an inordinate amount of compute resources, which has both financial and environmental implications.

**WHAT’S NEXT?**

OpenAI’s operating model attempts to provide a backbone from which to offer novel and innovative AI products and services that go far beyond its own offerings. As first to market, OpenAI has the ability to initially lock in customers and corner the potential market. From there, they will double down investment in the core technology to create a technical moat. While ChatGPT is enjoying the limelight, other LLMs (OPT – META, LAMDA – Google, Ernie Bot – Baidu and many others) are maneuvering their own chatbot services to slice out their share of the market. Expect an influx of entrants from big tech soon. As the playing field grows, so will the opportunities to partner with the newest players.

In addition to using ChatGPT and similar capabilities out of the box, many organizations may also achieve more value if they can train or finetune the models with domain-specific data. Several questions on data and model ownership and rights remain, but an important first step is understanding the high level process for using GPT models through extensive finetuning (see Booz Allen’s “LLMs: A Technical Primer”).

On February 21, 2023, Bain announced a global services alliance with OpenAI to help its clients realize value from AI advancements. Bain had already embedded OpenAI technologies into its internal knowledge manage systems to improve efficiency and are looking to expand those early successes more broadly.
About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology for more than 100 years. Today, the firm provides management and technology consulting and engineering services to leading Fortune 500 corporations, governments, and not for profits across the globe. Booz Allen partners with public and private sector clients to solve their most difficult challenges through a combination of consulting, analytics, mission operations, technology, systems delivery, cybersecurity, engineering, and innovation expertise.

To learn more, visit BoozAllen.com. (NYSE: BAH)