



NACo Tech Xchange Brief

CHATGPT



History

Per Wikipedia, ChatGPT^[a] is an [artificial-intelligence](#) (AI) [chatbot](#) developed by [OpenAI](#) and launched in November 2022. It is built on top of OpenAI's [GPT-3.5](#) and [GPT-4](#) families of [large language models](#) (LLMs) and has been [fine-tuned](#) (an approach to [transfer learning](#)) using both [supervised](#) and [reinforcement learning](#) techniques.

ChatGPT was launched as a prototype on November 30, 2022. It garnered attention for its detailed responses and articulate answers across many domains of knowledge.^[3] Its uneven factual accuracy, however, has been identified as a significant drawback.^[4] Following the release of ChatGPT, OpenAI's valuation was estimated at [US\\$29 billion](#) in 2023.^[5]

The original release of ChatGPT was based on GPT-3.5. A version based on GPT-4, the newest OpenAI model, was released on March 14, 2023, and is available for paid subscribers on a limited basis.

Problem Statement

What policies, guardrails, and usage guidelines need to be applied to the use of ChatGPT? ChatGPT has already succumbed to sensitive data exposure. [ChatGPT Exposed Payment Card Data of Subscribers \(govinfosecurity.com\)](#). It is also considered to be a major game changer, per Satya Nadella of Microsoft who claims **"this technology is going to reshape pretty much every software category"**.

Benefits

Given the concerns around ChatGPT, the insatiable interest and use of ChatGPT are already being realized by local government. Benefits realized so far include but are not limited to:

- Shortening research time
- Helping developers to write more efficient running code
- Providing an automated way to write infrastructure routines
- Helping improve written communications (i.e. letters, memos, emails, etc.)
- Providing templates for policies, job descriptions, etc
- Language translation

TIME IT TOOK TO REACH 100 million users:



MOBILE PHONE
16 YEARS



INTERNET
7 YEARS



FACEBOOK
4.5 YEARS



WHATSAPP
3.5 YEARS



INSTAGRAM
2.5 YEARS



TIKTOK
9 MONTHS



CHATGPT
2 MONTHS

ChatGPT is the fastest-growing consumer app in internet history.

Challenges

- **Data Privacy** – one needs to be very careful on what you are putting into ChatGPT. In a recent article in CSO, “Sensitive data currently makes up 11% of what employees paste into ChatGPT, with the average company leaking sensitive data to ChatGPT hundreds of times each week, according to Cyberhaven” Confidential information or personally identifiable information should not be part of the text you include.
- **Data Accuracy** – What is provided quickly is based on publicly available information through the internet. Fact checking is important as some of the information returned may be based on non-factual information.
- **Data Relevancy** – Currently ChatGPT only includes internet data from the fall of 2021. I expect this to change (if it hasn't already). But for now, it is important to be aware of this limitation.
- **Misuse** - potential misuse by malicious and criminal actors is already occurring. [Hackers](#) are already utilizing the bot to create more convincing malware or phishing scams, and the model could be tasked with creating and spreading misinformation.

County Perspectives

- Are approaching this new tool, with mixed reactions, as well as keen interest due to the obvious benefits.

- Have already used ChatGPT for interview questions, baseline code layouts, ansible playbooks (blueprint of automation tasks—which are complex IT actions executed with limited or no human involvement), memo layouts.
- Have voiced concerns around staff being mindful of what they are putting “in” to ChatGPT.

Recommended Strategies

- Develop a county policy on the use of AI (artificial intelligence) that is responsible and ethical. Content should include the county position on:
 - Privacy and data security
 - Transparency and accountability:
 - Fairness and bias:
 - Informed consent
 - Responsible use

More information clarifying each of these areas can be found at [What should ChatGPT's ethical use policy include in the context of the use of this technology in schools, colleges and universities? | ResearchGate](#)

- Educate staff on ChatGPT and how it can be used in a positive way, as well as what the pitfalls.
- Implement ChatGPT for county solution development through the [Azure OpenAI Service](#). It is available.

It gets you 70% of the way there, and you fill in the last 30%.

It's definitely a productivity multiplier. **For a real-life example:**

Staff needed to update DNS settings on 600 printers that are statically assigned.

What to Watch For

- As of this brief finalization, Italy has banned all Italian residents from accessing ChatGPT - [OpenAI geoblocks ChatGPT in Italy | TechCrunch](#), claiming that ChatGPT has violated European Union's General Data Protection Regulation (GDPR).
- The pace and feature improvements of newer versions of ChatGPT. [ChatGPT 4](#) is already out for subscribers to the paid version. It includes the ability to interpret images and respond in written form on how to use the image or what the image stands for

Resources:

[Knowledge versus wisdom: The dawn of ChatGPT \(naco.org\)](#)

<https://www.spiceworks.com/tech/artificial-intelligence/guest-article/chatgpt-active-directory-ad-security/>



COUNTY TECH
XCHANGE

For more information, visit:

County Tech Xchange (naco.org), or contact
Rita Reynolds, NACo CIO at rreynolds@naco.org