itihaasa
Research and Digital

ITIHAASA POINT OF VIEW

MARCH 2023

HOW TO ENSURE THE FAIR USE OF THE DATA THAT POWERS CONVERSATIONAL, GENERATIVE AI TOOLS LIKE CHATGPT

Kris Gopalakrishnan, N Dayasindhu and Krishnan Narayanan

A version of this viewpoint appeared in The Economic Times.[1]

OpenAI's ChatGPT has captured the world's imagination and sprinted to attract millions of users in a short time. ChatGPT states that it is an AI-powered chatbot developed by OpenAI, based on the GPT (generative pretrained transformer) language model. It uses deep-learning techniques to generate human-like responses to text inputs in a conversational manner. ChatGPT was trained using a dataset of hundreds of billions of words.

Microsoft has already announced a Bing + Edge powered by ChatGPT and GPT3.5 search that provides answers in a chat mode and can create new content or code. The new Bing + Edge is envisaged as an important arsenal in Microsoft's fight to improve its position in search — the most important software product market of this era.

While ChatGPT and conversational, generative AI is an exciting innovation that has caught the attention of users worldwide, it is not yet a silver bullet. Apart from other shortcomings, ChatGPT hallucinates as it imagines things which are not factual and shares those in a very convincing manner.

In all this excitement, what captured our attention is a news report that mentions that Microsoft may release a ChatGPT model-based solution to help private and public entities launch their own chat services. This is possible and meaningful only if these entities have collected data to train the ChatGPT model. Some experts are already exhorting entities to step-up data collection activities to train the ChatGPT model to offer domain-focused chat services. More important, this should happen in a policy context that protects data rights, and has robust mechanisms to anonymize and share personal data safely.

Possible use cases

The premise is that a ChatGPT model trained on domain specific data is better than a generic ChatGPT model to answer questions in that domain. Let us look at three India related sample use cases for conversational, generative AI services:

1. A government-run chat service that helps analyse data and text in public documents. These can include budget documents and economic surveys across multiple years, and various acts of parliament.
2. An in-company chat service for employees that helps to set up their BYOD (bring your own device) laptop, choose an office discussion room that is best suited for a meeting, categorise bills, and apply for reimbursement, etc.
3. A startup's monetised chat service that allows users to query product reviews written on multiple e-commerce sites and get answers to specific questions they have about a product's compatibility with other products, suitability of the product in a specific-use context, installation services, etc.

These are all valuable conversational, generative AI that enhance user satisfaction in many domains. Some of these domains are less complex. Other domains such as healthcare, education, and financial services may require rigorous sandbox testing and policy guardrails to ensure that these services provide acceptable levels of trustworthy and validated information.

1 https://economictimes.indiatimes.com/prime/technology-and-startups/how-to-ensure-the-fair-use-of-the-data-that-powers-conversational-generative-ai-tools-like-chatgpt/primearticleshow/98187055.cms

Policy and regulation

Does the demonstrated robustness till now make a compelling case for adopting domain-specific conversational, generative AI? It may seem so in the current exuberance. Conversational, generative AI has to become more robust, and there are good reasons to believe that it is on that path. Along with the evolution of AI models, there is also need to dive deeper into policies around data – the engine powering the domain knowledge of conversational, generative AI.

Three considerations pertaining to data require analysis and deliberation. This is especially important in India, where many are not savvy enough to understand the implications of data policies.
The first consideration is data rights. The government and its citizens collectively have rights over the data used for training the chat service in the first case. In the second case, the data is from a company's internal processes, and the chat service is for its own employees. In these two cases, the entities providing the chat service seem to have the data rights that power the service. There is a low probability of third-party conflicts in using the data.

In the third case, the customer reviews data is likely to include personal details of customers of various e-commerce companies. The e-commerce companies may need to get explicit permission from customers who have provided reviews to anonymise, share, and monetise such data with a third-party chat-services startup. There should be an option for their customers to opt out of the anonymisation and sharing process if they wish so. This implies that there should be policies to protect the data rights of individuals.

The second consideration is anonymising personal data. Anonymisation is the irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, and such a process conforms to appropriate standards of irreversibility. Government policies are evolving to set up appropriate standards for anonymisation and identify penalties when there are wilful breaches in anonymisation.

The third consideration is data sharing in the context of public good. When the government wants to build a public chat service that includes data from private entities and individuals, there needs to be institutional mechanisms to help private entities and individuals share non-personal data and anonymised personal data. Even in the context of public good, the private entities holding personal data of individuals may need to get the explicit consent of individuals before sharing their anonymized data. While the data may be free, there may be costs incurred to store and anonymise the data, for which private entities may need to be compensated for.

So far, Indians have been generous is sharing their data with different digital platforms that have monetised services based on this data. Going forward, we should address the following question: What is the institutional mechanism to govern data sharing by individuals and the community with private entities and the government?

All these aspects related to data rights, anonymisation, and data sharing are analysed in the report submitted by the committee set up by MeitY on a data governance framework focussing on non-personal data. MeitY has also published a robust draft data-governance framework policy that balances the non-personal data use and data protection.

There is a need to embrace the advances that may make technologies like conversational, generative AI more accessible to all Indians while maintaining the sanctity of data rights, recommending standards for anonymising personal data, and identifying appropriate mechanisms of data sharing. This will make the use of technology innovations like conversational, generative AI a win-win for citizens, government, and private entities.

***