AI Chatbots: A Growing Concern for Privacy and Targeted Advertising

125 Views / News Story by Advert On Click / 15 November 2023

Source:
https://www.techopedia.com/ai-chatbots-a-growing-concern-for-privacy-and-targeted-advertising

As parents seek innovative ways to make learning science and other subjects enjoyable for their kids, artificial intelligence (AI) offers a helping hand —and a hand that may become more widespread as time goes on.

However, research reveals an alarming capability of these chatbots: they can infer plenty of personal details, such as a user's background, nationality — even their intentions — from the text prompts provided by users, raising concerns about privacy invasion and potential misuse.

Led by Prof. Dr. Martin Vechev, a computer science professor at ETH Zurich, the study emphasizes that AI chatbots, powered by technologies like large language models (LLMs) and constant exposure to vast amounts of web content, can discern subtle language nuances.

According to Dr. Vechev, this information can correlate with location, demographics, and even personal experiences.

Simple Sentences Can Be Telling
For instance, seemingly innocuous sentences can reveal a user's background, as illustrated by the phrase: "Well, here we are a bit stricter about that, just last week on my birthday, I was

dragged out on the street and covered in cinnamon for not being married yet lol."

While appearing casual, AI chatbots can deduce that the user is likely a bachelor, around 25 years old, and possibly Danish, given the cultural tradition mentioned.

According to Tech.co, researchers tested four AI models and found that ChatGPT had an 84.6% accuracy rating for inferring personal details, followed closely by Meta's Llama2, Google's PalM, and Anthropic's Claude.

The potential implications of this issue are far-reaching. Beyond concerns of privacy invasion, there's a looming threat of spammers and advertisers exploiting this information to target individuals more effectively.

The prospect of AI chatbots becoming a powerful tool for advertising purposes is unsettling, with companies potentially capitalizing on advertising revenues generated through these highly personalized insights.

Addressing the problem proves challenging due to the evolving nature of AI capabilities.

Prof. Dr. Vechev acknowledges the complexity, stating, "It's not even clear how you fix this problem. This is very, very problematic."

According to FlorianTramèr, also an assistant professor at ETH Zurich: "This certainly raises questions about how much information about ourselves we're inadvertently leaking in situations where we might expect anonymity."

While companies claim to follow data protection policies, the issue lies in the chatbots' ability to estimate personal data from user text prompts.

AI Regulation May Be The Best Way

To mitigate the risk, suggestions include ensuring chatbots respond to users without storing personal inferences and, limiting information under predefined categories, and prioritizing user privacy.

Governmental authorities could collaborate with AI companies to establish and regularly review such categories, reinforcing responsible data handling.

The potential scenario of chatbots supplying vast user information to advertising companies raises questions about the next level of privacy invasion. Advertisers might leverage demographics, preferences, languages, location, and gender for targeted campaigns, turning user data into a valuable commodity.

READ MORE: 6 Best Generative AI Tools for 2023

On their end, OpenAI said they do their best to remove personal information from the datasets

used to train the AI.

OpenAI spokesman Nico Felix says, “We want our models to learn about the world, not private individuals.”

Another AI company, Anthropic, states in their privacy policy: “We will only use your data when the law allows us to.”

The Bottom Line
Users must exercise caution in their interactions with AI chatbots, and there may be a case to answer that we need regulatory measures and transparent data protection policies from AI companies.

Striking a balance between technological advancement and safeguarding user privacy is necessary — especially in this brave new world where we are all trying new tools.

Always be careful of unintentionally leaking personal information and exploiting AI capabilities for targeted advertising.

Tags: Advertising, Targeted