Artificial intelligence expert weighs in on the rise of chatbots

March 17 2023, by Joe McAdory

Credit: Pixabay/CC0 Public Domain

What if a chatbot comes across as a friend? What if a chatbot extended what could be perceived as intimate feelings for another? Could chatbots, if used maliciously, pose a real threat to society? Santu Karmaker, assistant professor in computer science and software engineering, took a deep dive into the subject below.

What do these odd encounters with chatbots reveal about the future of AI?

Karmaker: It does not reveal much because the future possibilities are infinite. What is the definition of an odd encounter? Assuming that "odd encounter" here means the human user feels uncomfortable during their interaction with the chatbots, we are essentially talking about human feelings/sensitivity.

There are two important questions to ask: (1) Don't we have odd encounters when we converse with real humans? (2) Are we training AI chatbots to be careful about human feelings/sensitivity during conversations?

We can do better, and we are making progress regarding equity/fairness issues in AI. But it's a long road ahead, and currently, we do not have a robust computational model for simulating human feelings/sensitivity, which is why AI means "artificial" intelligence, not "natural" intelligence, at least yet.

Are companies releasing some chatbots to the public to soon?

Karmaker: From a critical point of view, products like ChatGPT will never be ready to go unless we have a working AI technology that supports continuous life-long learning. We live in a continually evolving world, and our experiences/opinions/knowledge are also evolving. However, current AI products are trained mostly on a fixed historical data set and then deployed in real life with the hope that they can generalize to unseen scenarios, which often does not turn out to be true. However, much research is now focusing on life-long learning, but the field is still in its infancy.

Further, technology like ChatGPT and life-long learning have orthogonal goals, and they complement each other. Technology like ChatGPT can reveal new challenges for life-long learning research by receiving feedback from the public on a large scale. Although not quite "ready to go," releasing products like ChatGPT can help gather large amounts of qualitative and quantitative data for evaluating and identifying the limitations of the current AI models. Therefore, when we are talking about AI technology, whether a product is indeed "ready to go," is highly subjective/debatable.

If these products are released with many glitches, will they become a societal issue?

Karmaker: Glitches in a [chatbot](link)/AI system differ greatly from regular software glitches we normally refer to. A glitch is usually defined as an unexpected behavior of a software product being used. But what is a glitch for a chatbot? What is the expected behavior?

I think the general expectations from a chatbot are that the conversations should be relevant, fluent, coherent, and factual.

Clearly, any chatbot/intelligent assistant available today is not always relevant, fluent, coherent, and factual. Whether this will become an issue of social concern mostly depends on how we deal with such technology as a society. If we promote human-AI collaborative frameworks to benefit from the best of humans and machines, that will mitigate the societal concerns of glitches in AI systems and, at the same time, increase the efficiency and accuracy of the goal task we want to perform.

Lawmakers seem hesitant to regulate AI. Could this change?

Karmaker: I don't see a change in the near future. As AI technology and research are moving at a very fast speed, a particular product/technology becomes obsolete/old-fashioned very quickly. Therefore, it is really challenging to accurately understand the limitations of such technology within a short time and regulate such technologies by creating laws. Because by the time we uncover the issues with AI technology at a mass scale, new technology is being created, which shifts our attention from the previous ones towards the new ones. Therefore, lawmakers' hesitation to regulate AI technology might continue.

What are your biggest hopes for AI?

Karmaker: We are living in an information explosion era. Processing a large amount of information quickly is not a luxury anymore; rather, it has become a pressing need. My biggest hope for AI is that it will help humans process information at a large scale and speed and, therefore, help humans make better-informed decisions that can impact all aspects of our life, including healthcare, business, security, work, education, etc.

There are concerns AI will be used to produce widespread misinformation. Are those concerns valid?

Karmaker: We have had cons since the dawn of society. The only way to deal with them is to identify them quickly and bring them to justice. One key difference between traditional crime and cybercrime is that it is much harder to identify a cybercriminal than a regular one. This identity verification is a general problem with internet technology, rather than only being specific to AI technology.

AI technology can provide cons with tools to spread misinformation, but if we can identify the source quickly and capture the cons behind it,

spreading misinformation can be stopped. Lawmakers can prevent a catastrophic result by: (1) enforcing strict license requirements for any software which can generate and spread new content on the internet; (2) creating a well-resourced cybercrime monitoring team with AI experts serving as consultants; (3) continuously providing verified information on the GOV/trusted websites, which will allow the general people to verify information from sources they already trust; and (4) making basic cybersecurity training required and making educational materials more accessible to the public.

Provided by Auburn University at Montgomery