Opinion

ChatGPT: Legal implications of algorithmic bias and consumer privacy

By Dr Sia Chin Chin / Taylor's University

17 May 2023, 11:33 am

Dr Sia Chin Chin is the programme director for Master of Laws Programme and senior lecturer at Taylor's Law School, Faculty of Business and Law, Taylor's University.

The release of ChatGPT less than six months ago has demonstrated to us the seemingly powerful capabilities of generative artificial intelligence (AI), which can grasp a gigantic amount of information and then construct new, original content after receiving a prompt from any registered user.

The dream of generating original content for our personal and professional use with simple prompts to a chatbot has now become a reality. In a jiffy, everyone is capable of writing computer codes, sophisticated emails, coursework papers, business reports or plans, poems, jokes, and even composing music or producing images!

Despite the strengths being emphasised, ChatGPT, which is based on large language learning models (LLMs), is a double-edged sword and has several limitations. The wanton usage of it is likely to lead to undesired main legal implications, namely algorithmic bias and consumer privacy.

Algorithmic bias

Algorithmic bias can exhibit itself in numerous ways with varying degrees of consequences for the subject group within the community of users. It is crucial to remember that the most challenging part with algorithmic bias is that, unlike human bias, it is very likely to spread like wildfire. A tiny bit of bias in data can lead to an enormous ripple effect.

In recognition of this reality, the American Bar Association, already in 2019, issued a resolution urging courts and lawyers to address the emerging ethical and legal issues related to the use of AI, including the technology of LLMs employed in ChatGPT.

In the European Union, in February this year, the lead lawmakers on the Artificial Intelligence Act, Brando Benifei and Dragos Tudorache, proposed that AI systems generating complex texts without human oversight should be part of the "high-risk" list, to prevent ChatGPT from churning out disinformation at scale.

In Australia, in March this year, a regional Australian mayor said he may sue OpenAI if it does not correct ChatGPT's false claims that he had served time in prison for bribery, in what would be the first defamation lawsuit against the automated text service. Brian Hood, who was elected mayor of Hepburn Shire, became concerned about his reputation when members of the public told him ChatGPT had falsely named him as a guilty party in a foreign bribery scandal involving a subsidiary of the Reserve Bank of Australia in the early 2000s. Lawyers for Hood sent a letter of concern to ChatGPT owner OpenAI on March 21, giving the company 28 days to fix the errors.

Consumer privacy

Developing technology with the ability to generate new contents to users, such as ChatGPT, relies on a huge analysis of personal information. This triggers a variety of data privacy risks for users, for example:

Transparency and consent: Are people aware of how their information is being used to develop and used in technology? Have they consented to its use, or will their information be anonymised? Are the current thresholds for obtaining user consent (i.e., to be specific and informed, as well as minors) achievable given AI's complexity, uncertainty, and potential unpredictability?

Early April this year, Italy's Data Protection Authority temporarily banned ChatGPT chatbot and launched a probe over a suspected breach of the AI application's data collection rules. The agency, also known as Garante, accused ChatGPT of failing to check the age of its users who are supposed to be 13 and above. Garante claimed that ChatGPT has an "absence of any legal basis that justifies the massive collection and storage of personal data of users" to "train" the chatbot.

Recommendations

It is already a reality that the impact of LLMs such as ChatGPT is expected to grow in the foreseeable future. Other potential legal issues include the emergence of "dark LLMs", which may be hosted on the dark web to provide a chat bot without any safeguards, as well as LLMs that are trained on perhaps particularly harmful data.

Therefore, it is instrumental that the policy makers and law enforcement community prepare for how its positive and negative applications may affect their daily businesses. Law enforcement officers need to start developing the skills necessary to make the most of models such as ChatGPT. This means understanding how these types of systems can be leveraged to build up knowledge, expand existing expertise, and understand how to extract the required results.

This will imply that officers need to be able to assess the content produced by generative AI models in terms of accuracy and potential biases. With the progress of technology, and new models becoming available, it will be increasingly important for law enforcement to stay at the forefront of these developments to anticipate and prevent abuse, as well as to ensure potential benefits can be taken full advantage of.

Dr Sia Chin Chin is the programme director for Master of Laws Programme and senior lecturer at Taylor's Law School, Faculty of Business and Law, Taylor's University.