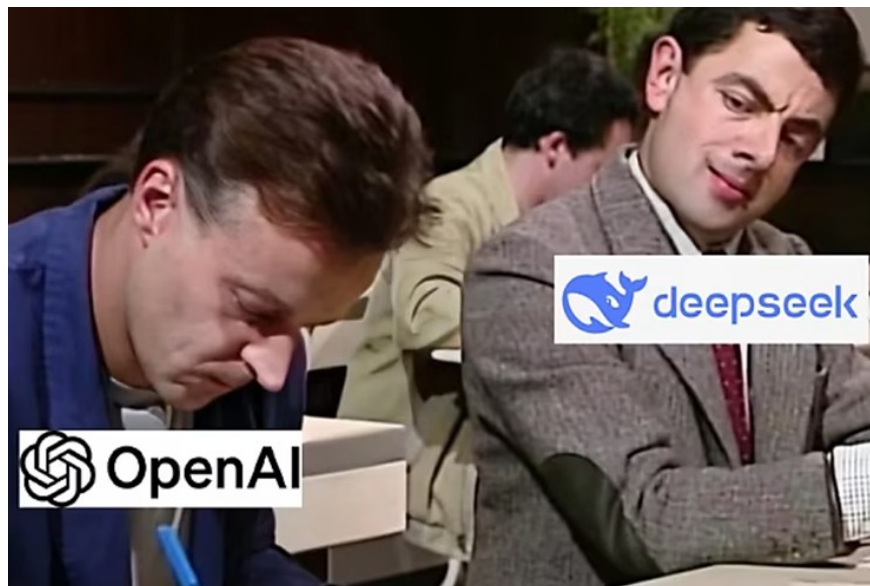


Decoding the 'distillation' technique that brought DeepSeek success

The success of Chinese AI startup DeepSeek has led to a concept called 'distillation'.

Since DeepSeek released its powerful large language model called R1, it has created waves across Silicon Valley and the US stock market, causing widespread discussion and debate.



DeepSeek used distillation without asking OpenAI for permission?

University of Michigan (USA) statistics professor Ambuj Tewari, a leading expert in AI and machine learning, shared his insights on the technical, ethical, and market aspects involved in DeepSeek's breakthrough.

What is the distillation technique that OpenAI accuses DeepSeek of using?

OpenAI has accused DeepSeek of using a technique called 'model distillation' to train its own models based on OpenAI's technology. But what does this mean? Essentially, model or knowledge distillation typically involves creating feedback from a stronger model to train a weaker model in order to help the weaker model improve.

This is a perfectly normal practice if the more powerful model is released with a license that allows such use. But OpenAI's ChatGPT terms of use explicitly prohibit using their model for purposes like model distillation, so if DeepSeek is doing this, it would be in violation of AI development regulations.



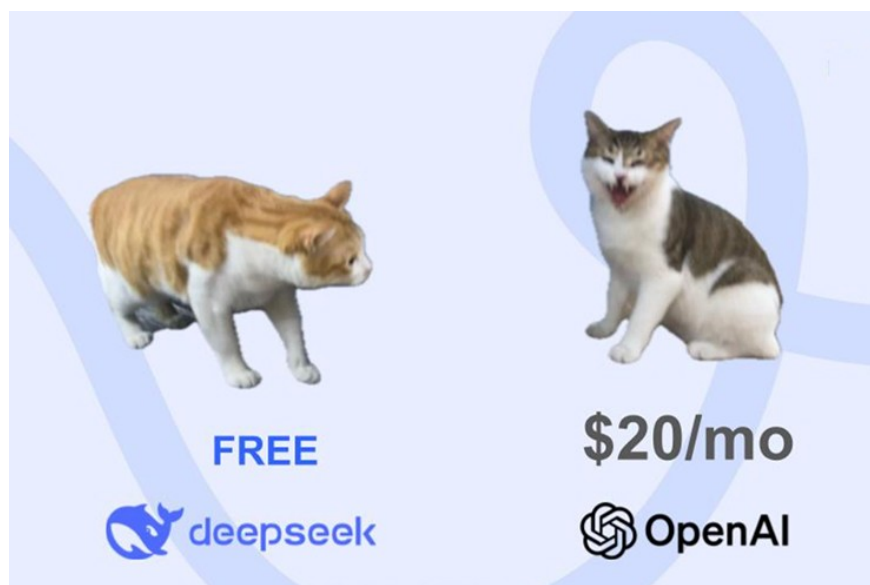
In addition to OpenAI, DeepSeek can also 'distill' knowledge from other AI-based inference engines.

Can DeepSeek use other open source models?

Even if DeepSeek uses distillation, they are not necessarily violating the rules. This happens if DeepSeek uses other open source models, such as Meta Platforms' LLaMA or Alibaba's Qwen, to distill knowledge without relying on OpenAI's proprietary model.

The fact that DeepSeek is not necessarily breaking the rules stems from the fact that even within the same model family, such as LLaMA or Qwen, not all models are released under the same license. If a model's license allows distillation of the model, then there is nothing illegal or unethical about doing so.

Interestingly enough, in an ArXiv analysis of DeepSeek R1, AI experts mention that this process actually works in reverse, with knowledge being distilled from R1 into LLaMA and Qwen to enhance the reasoning capabilities of later models.



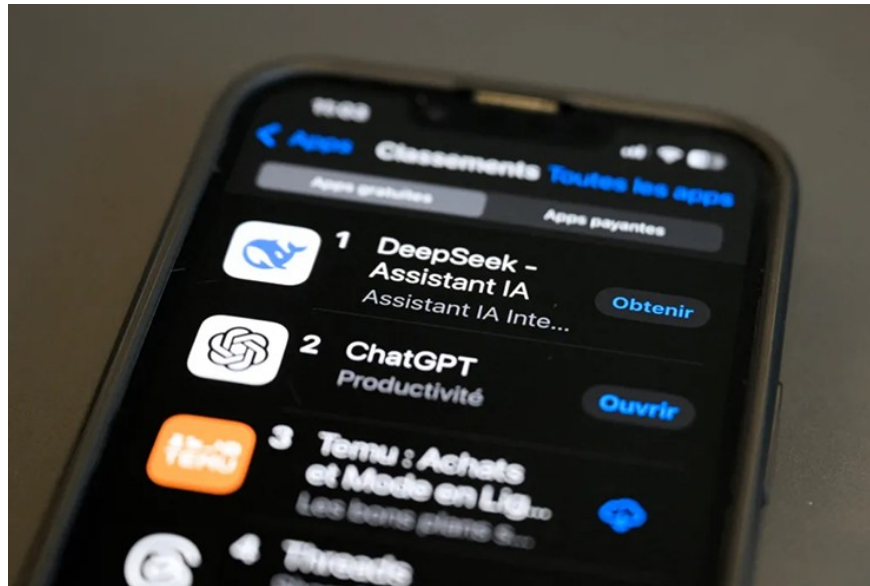
Using distillation techniques makes DeepSeek's operating costs much cheaper.

How does DeepSeek prove their model was developed independently?

Since there is speculation about DeepSeek's violation, the burden of proof will be on OpenAI to show that DeepSeek actually violated their terms of service. This is a difficult task because only the final model developed by DeepSeek is public, not its training data, so it is difficult to prove the accusation. Since OpenAI has not yet made its evidence public, it is difficult to say whether their argument against DeepSeek is correct.

Are there any standards to ensure that AI development is not violated?

There are currently few widely accepted standards for how companies develop AI models. Advocates of open models argue that openness leads to greater transparency. But opening up model weights is not the same as opening up the entire process, from data collection to training. There are also concerns about whether using copyrighted material like books to train AI models constitutes fair use. A prominent example is the lawsuit filed by The New York Times against OpenAI, which highlights the legal and ethical debates around this issue.



It's unclear how DeepSeek works at this point, but it's still the most downloaded free app on the App Store.

There are questions around how social bias in training data affects model outcomes. There are also concerns around growing energy demand and its impact on climate change. Most of these issues are actively debated with little consensus.

Could DeepSeek pose the risk to US security that US officials fear?

According to Professor Ambuj Tewari, it would be very worrying if the data of American citizens was stored on DeepSeek's servers and the Chinese government had access to that data. However, the model weights are open, so the data could also be run on servers owned by American companies. In fact, Microsoft has already started hosting DeepSeek's models.

You finished reading the article "**Decoding the 'distillation' technique that brought DeepSeek success**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
