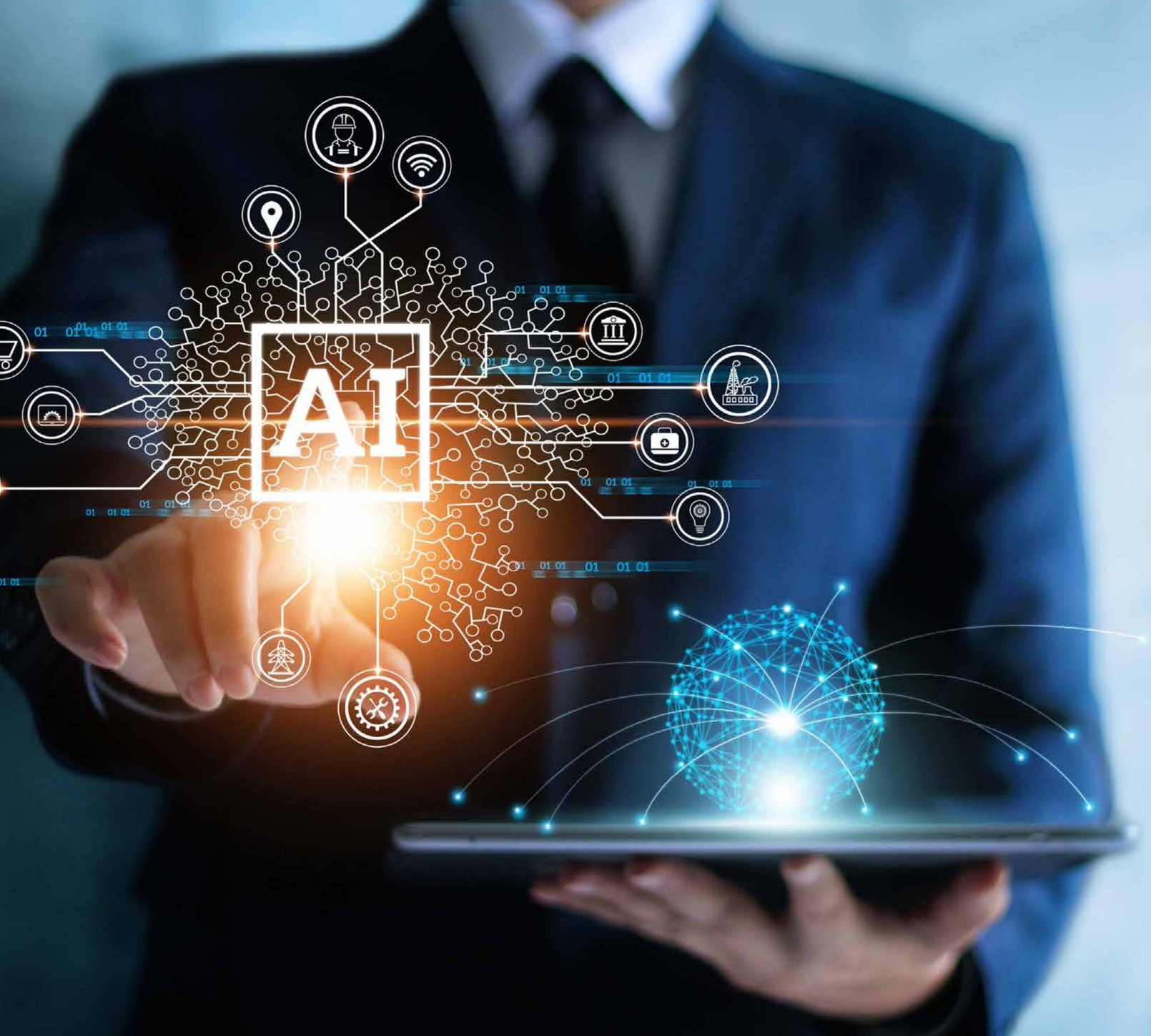


ERROL SCHMIDT

30 JULY 2024

The Training Trap: How AI Uses Your Data?

reinteractive
CONFIDENT SOFTWARE

What is AI?

- AI is any computer system that is designed to mimic human like thinking in some aspect.
- Generative AI is an AI application that can produce human like responses in the form of text, images, sound or video from a plain language prompt.

reinteractive
CONFIDENT SOFTWARE

What is AI?

- A Neural Network is a series of pieces of information linked together in a way that is similar to the way a brain works.

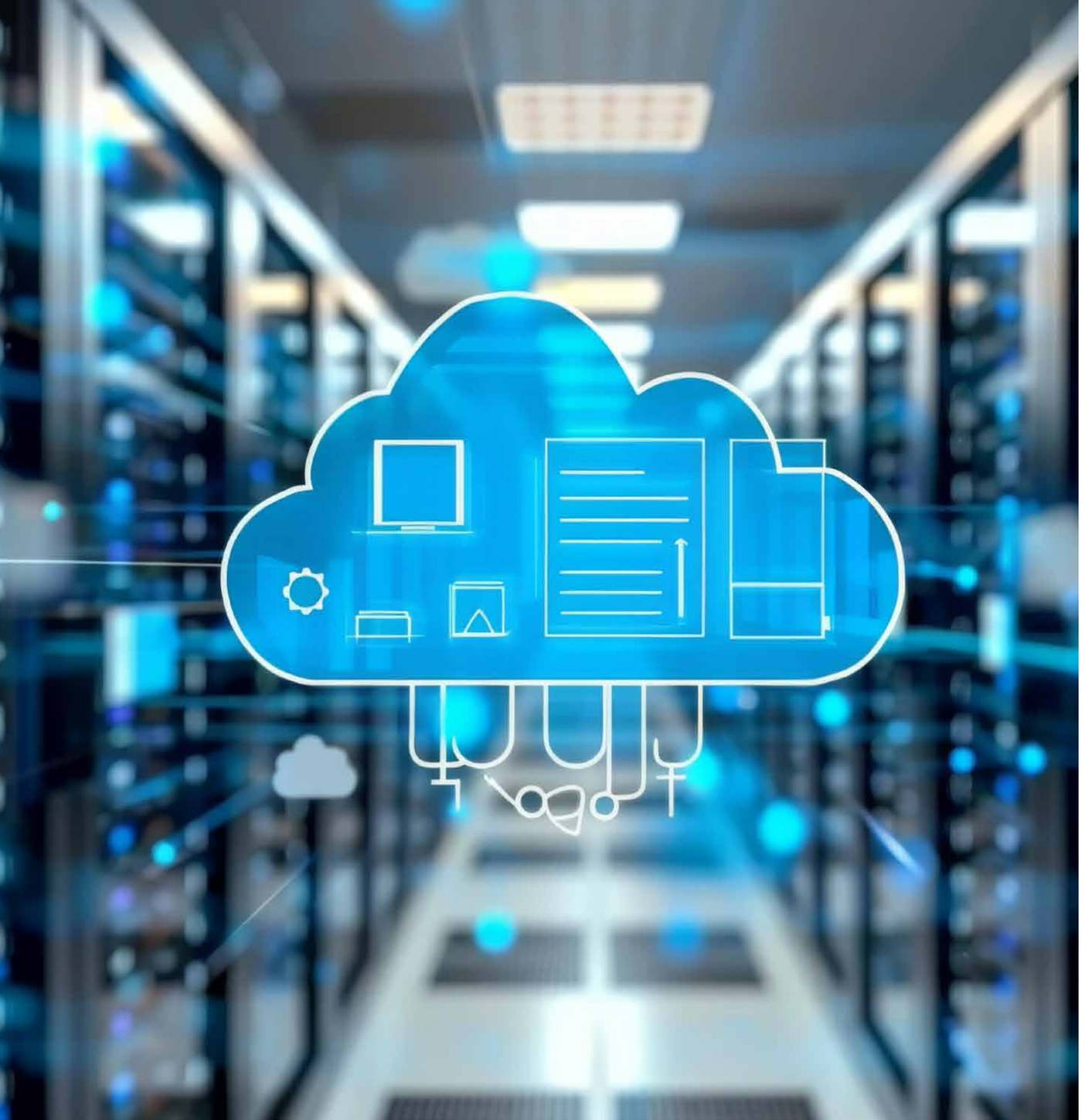
- A Neural network is the process by which a Gen AI model learns. It does this by going over training data many times (may be thousands) until the predicted media closely matches the actual learning data.

- This produces the Large Language Model.

reinteractive
CONFIDENT SOFTWARE

How does AI learn?

- It iterates over data many times over until the predicted output closely matches the actual data set.
- Fine tuning is the process of making adjustments to an LLM appropriate to your specific data.
- In this way an LLM can produce results specific to your dataset using what it knows about sentence structure and being understood.



How might it use your data?

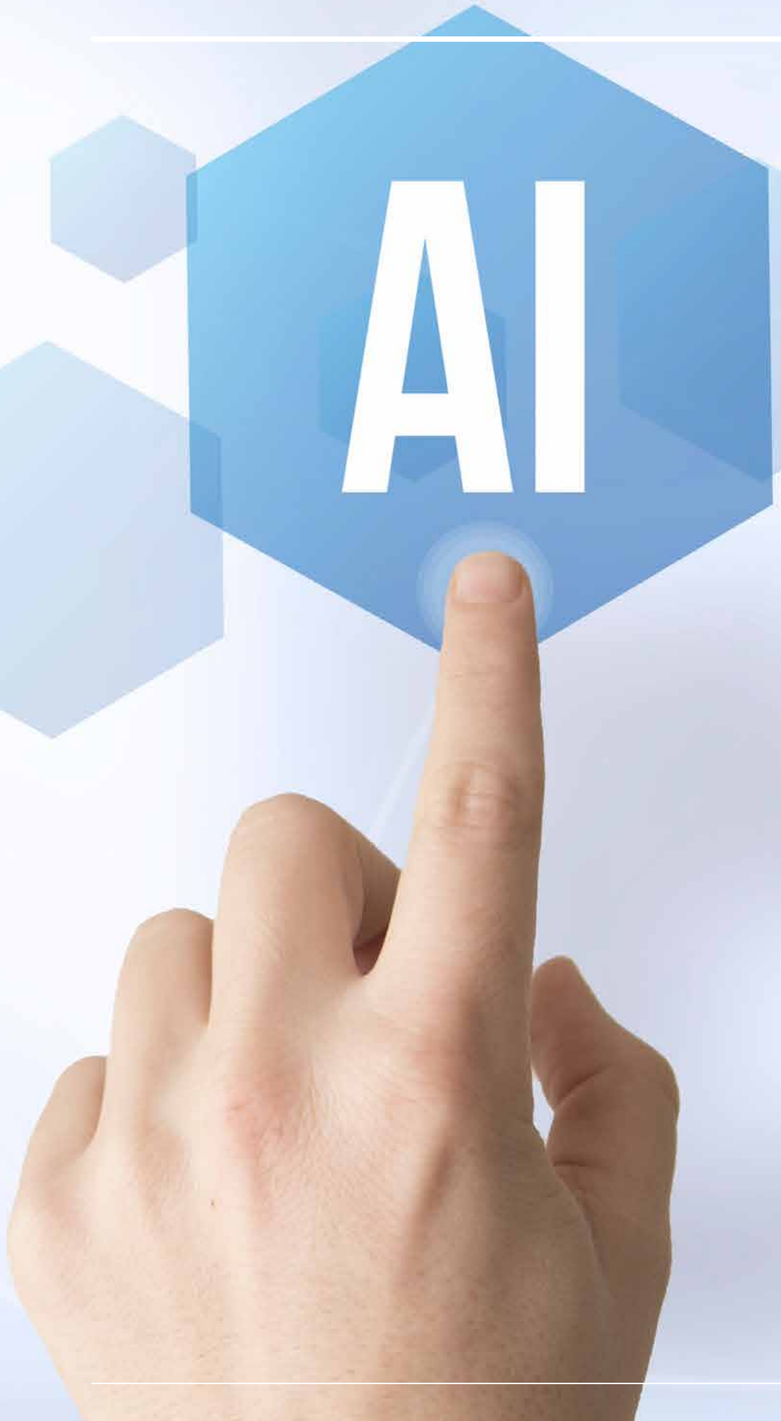
- One of the great advances that has made LLM's as capable as they are is access to a vast trove of data - that is everything that is publicly available on the internet.
- In order to become better at what it does it needs more data.
- Google has been digitising books and using CAPTCHA for many years as part of this.

reinteractive
CONFIDENT SOFTWARE

How might it use your data?

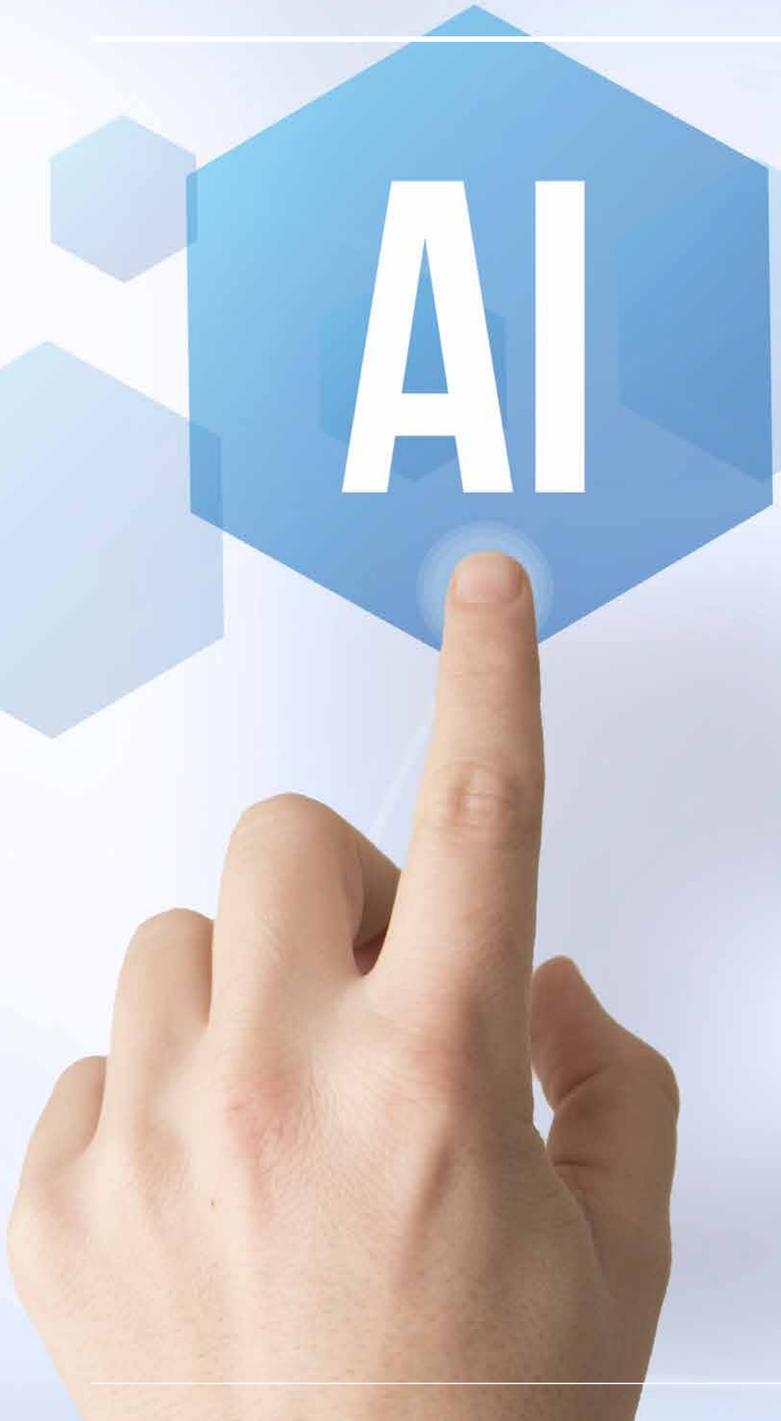
- There is an enormous amount of money and power available to the company that produces the best AI that is closest to human thinking.
- You may be right if you think that something undisclosed might go on.
- Given that you might not have known how LLMs were learning before, what might they be doing today that you might not know about?

reinteractive
CONFIDENT SOFTWARE



What is the risk?

- Proprietary data and personal information is all the same to a neural network trying to understand more and more.
- It can not distinguish the relevance or security factor in the same way that you can.
- A programmer instructing an LLM on what to do with a piece of information may not specify exactly enough what to do with this type of information.

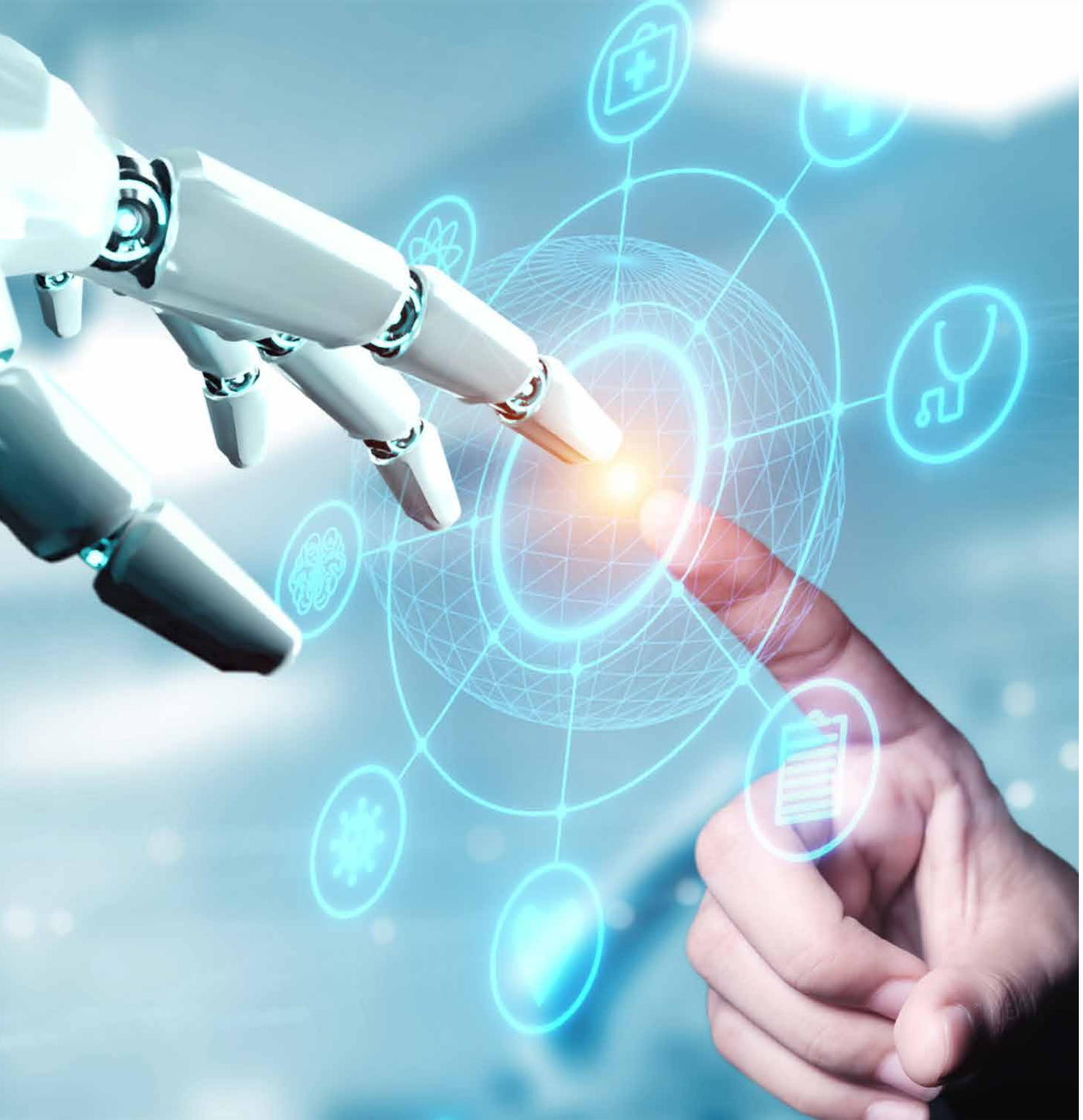


What is the risk?

- When a large corporate says ‘we promise to not use your data to teach our LLM’ should you believe them?
- Your data may show up in someone else’s results.

Overall:

While feeding a PDF into a general LLM doesn't automatically make it part of the model's learned data, it can influence its responses. The exact way this influence occurs depends on the specific model and its capabilities.

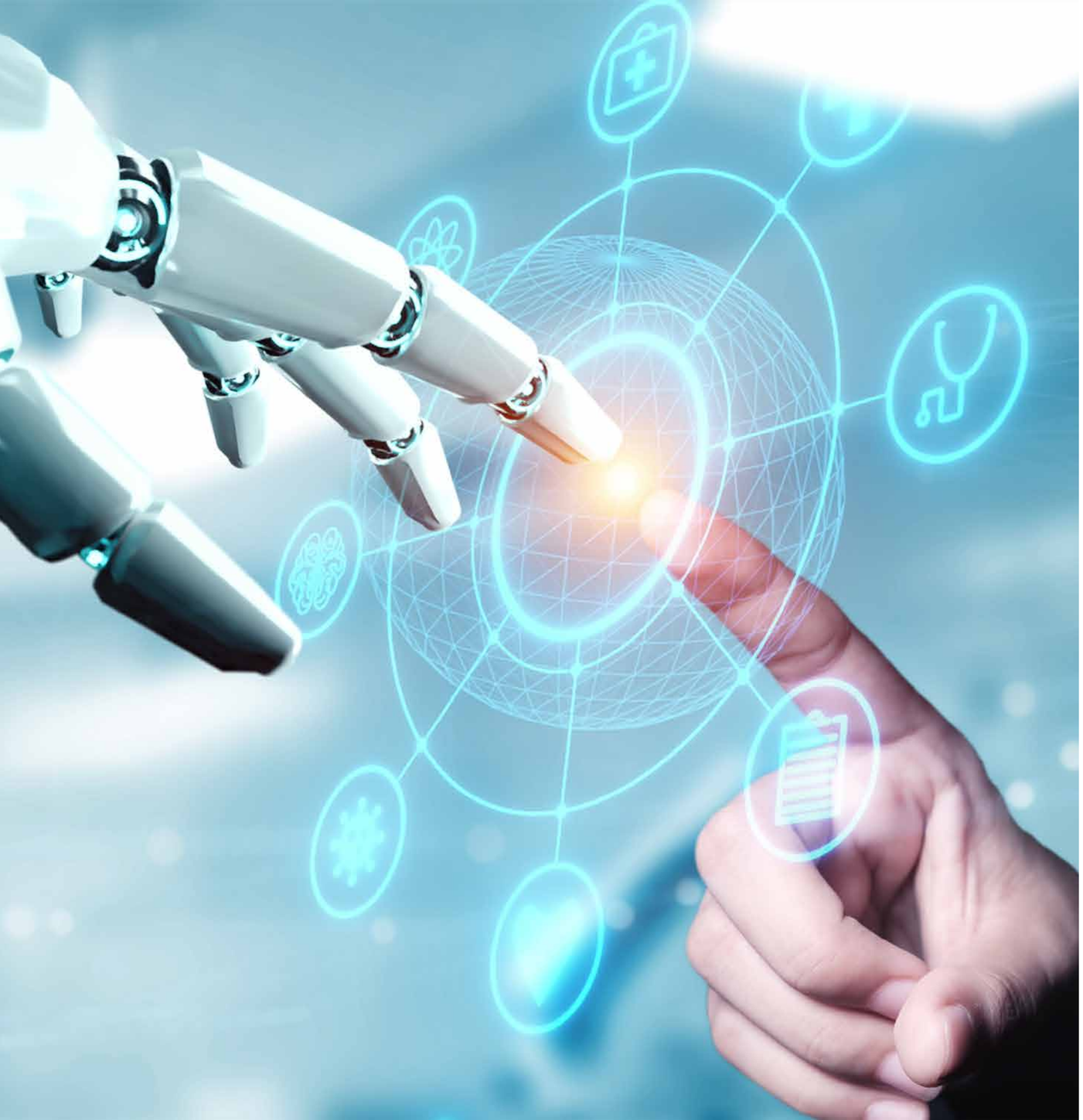


How to solve this

- **Don’t** input your proprietary information or personal information into a prompt, or provide to an LLM for further learning.

- **Don’t** use ‘off the shelf’ gen AI tools in a business setting where it may have access to such information (as appealing as this could be).

reinteractive
CONFIDENT SOFTWARE



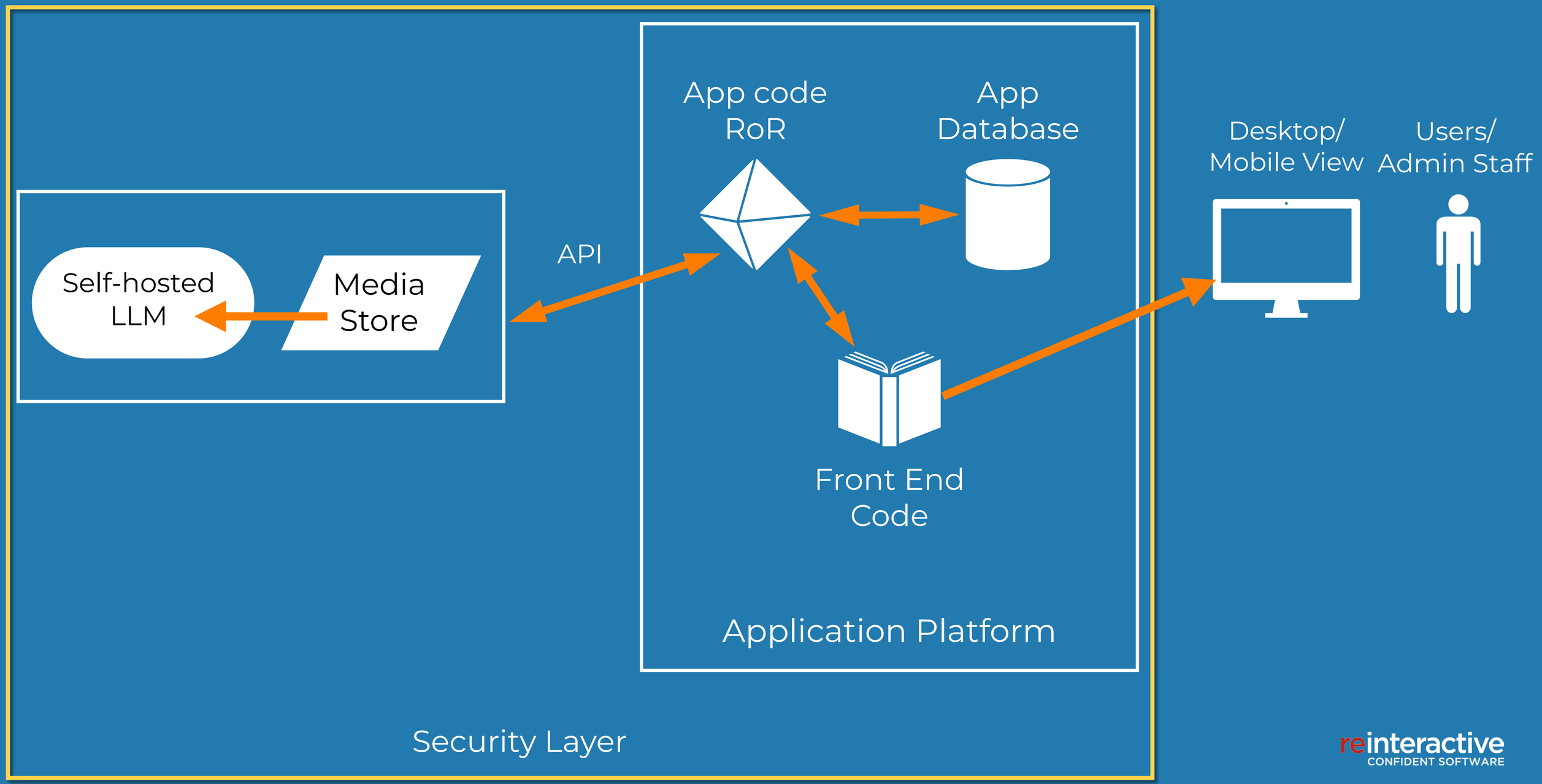
How to solve this

- If necessary, use only tools that are enterprise grade, meaning that they are guaranteed to be encrypted, secure, and where possible de-identify information before sending it to be processed (you will pay a bit more for this).

- The best solution is to host your own LLM and fine tune it your self.

reinteractive
CONFIDENT SOFTWARE

Architecture



reinteractive
CONFIDENT SOFTWARE

KOLLARAS
Trading Company

- Real world business application based on the above diagram.
- Application hosted on Heroku.
- Self-hosted LLm on AWS bedrock, with data hosted in S3.
- Serves the output to staff without concern for where that data sits.
- All within a secure boundary.

reinteractive
CONFIDENT SOFTWARE

Book a meeting with me

Book a time with me to discuss how reinteractive can deilver value to your business.

Scan the URL code and book your preferred time slot!

reinteractive
CONFIDENT SOFTWARE

Errol Schmidt CEO

+61 481-065-451

errol.schmidt@reinteractive.com

reinteractive.com