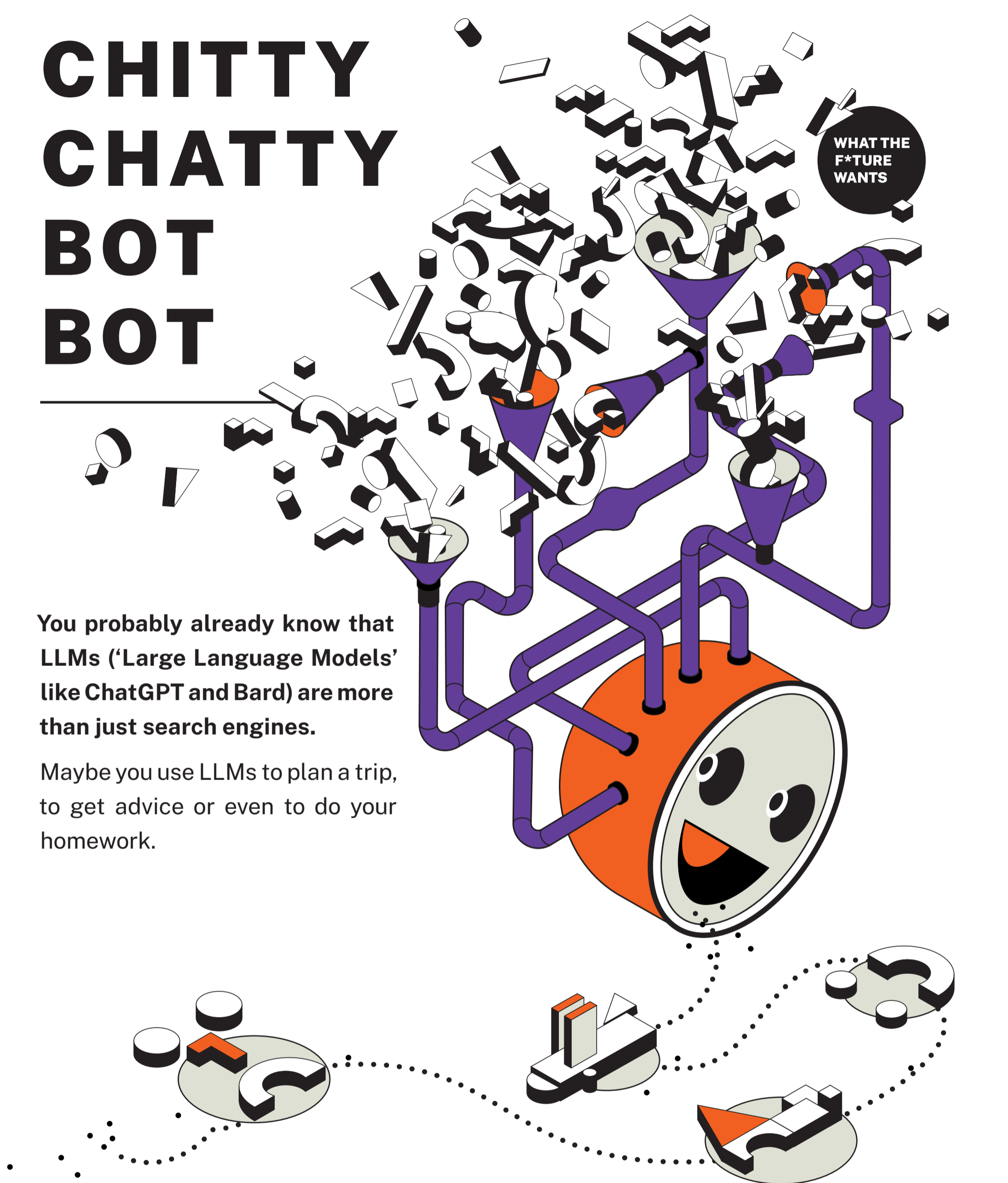# CHITTY CHATTY BOT BOT

You probably already know that LLMs ('Large Language Models' like ChatGPT and Bard) are more than just search engines.

Maybe you use LLMs to plan a trip, to get advice or even to do your homework.

These AI chatbot systems can be helpful… but they're far from perfect. While they may seem like an 'everything tool,' it's good to know what they're best at and where they fall short.

Find out how LLMs are built and how they work — and then you can decide how much you want to rely on them.
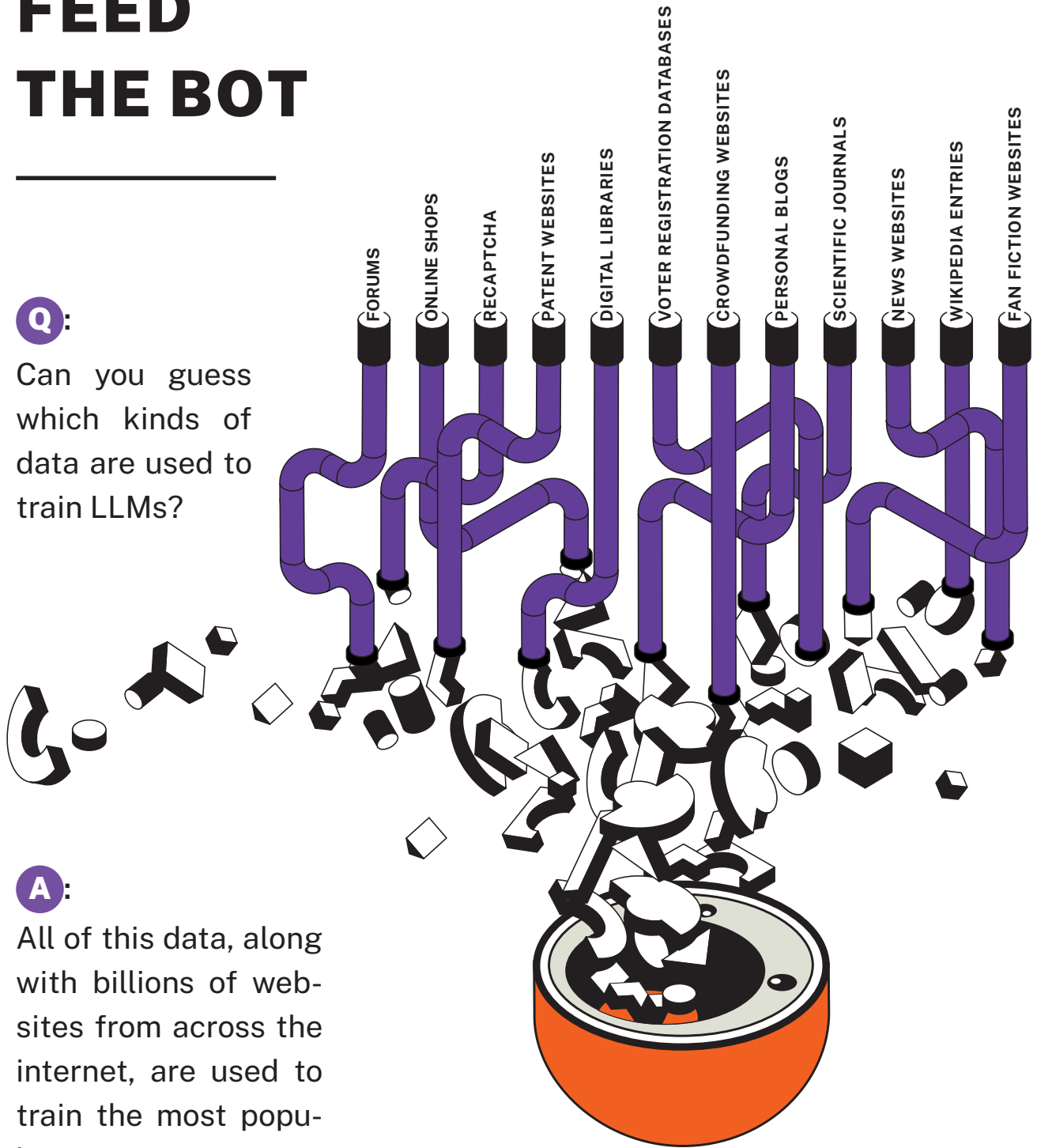
TACTICAL TECH

FEED
THE BOT

Q:

Can you guess which kinds of data are used to train LLMs?

A:

All of this data, along with billions of websites from across the internet, are used to train the most popular LLMs.

FORUMS

ONLINE SHOPS

RECAPTCHA

PATENT WEBSITES

DIGITAL LIBRARIES

VOTER REGISTRATION DATABASES

CROWDFUNDING WEBSITES

PERSONAL BLOGS

SCIENTIFIC JOURNALS

NEWS WEBSITES
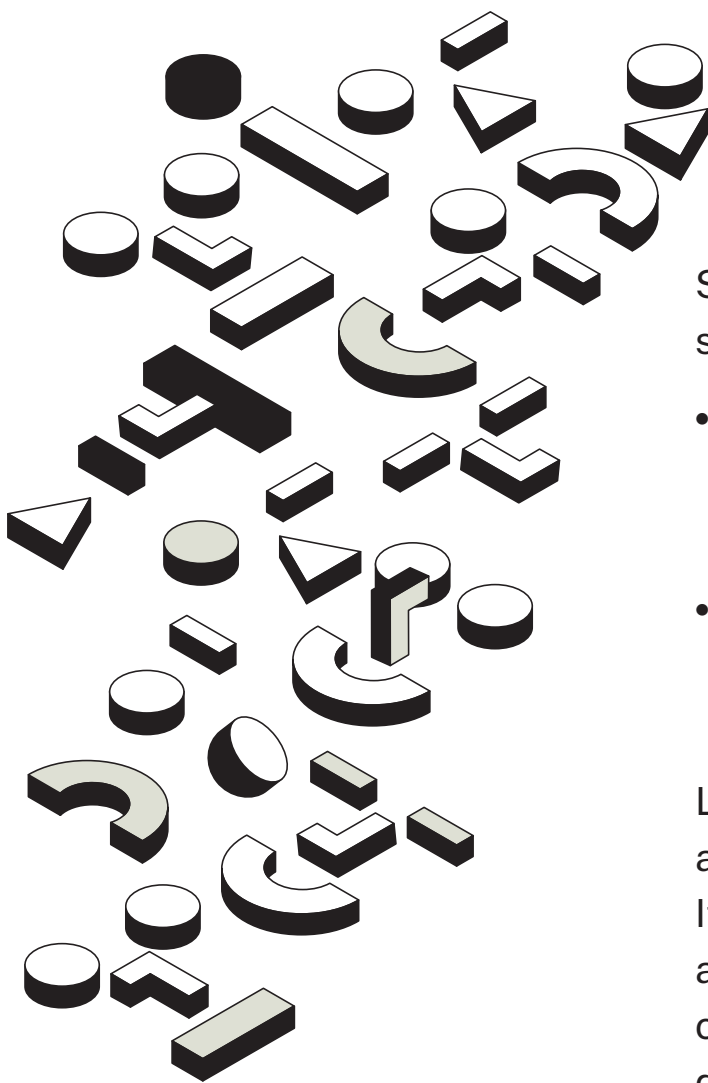
WIKIPEDIA ENTRIES

FAN FICTION WEBSITES

But before this data can be useful for training the LLM, it has to be labelled and categorised by loads of human workers.

GARBAGE IN, GARBAGE OUT

While it may seem like LLMs know everything on the internet, that doesn't make them all-knowing. Here are some reasons why:

- Some of the data they are trained on might be **personal**, copyrighted or used without permission.

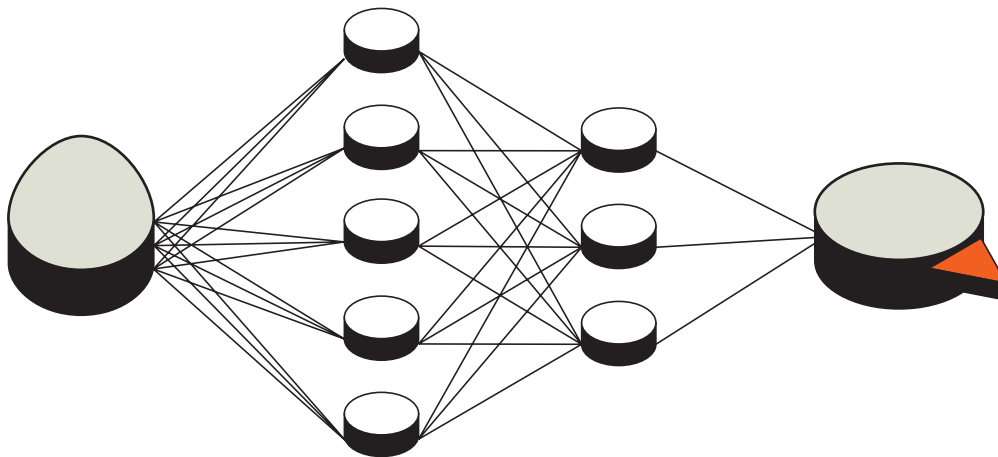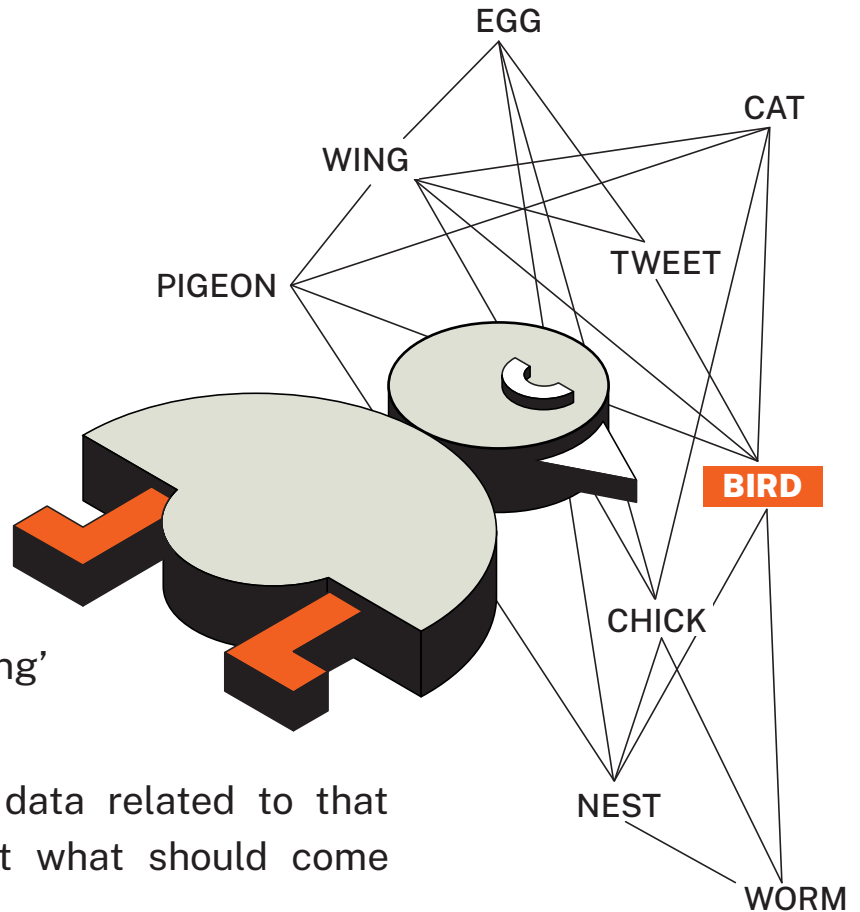Still not that bad? Well, those data sets might *also* be:

- Full of hate speech, conspiracy theories or information that is just **plain wrong**.

- **Biased** against certain jobs, cultures, religions, genders, or circumstances.

LLMs are trained on data that also leaves stuff out altogether. If there's little or no information about a group of people, language or culture in the LLM's training data, it won't be able to generate any answers about them.

WTF LLM?

How does the model 'learn' from data? Well, it's kind of like auto-complete:
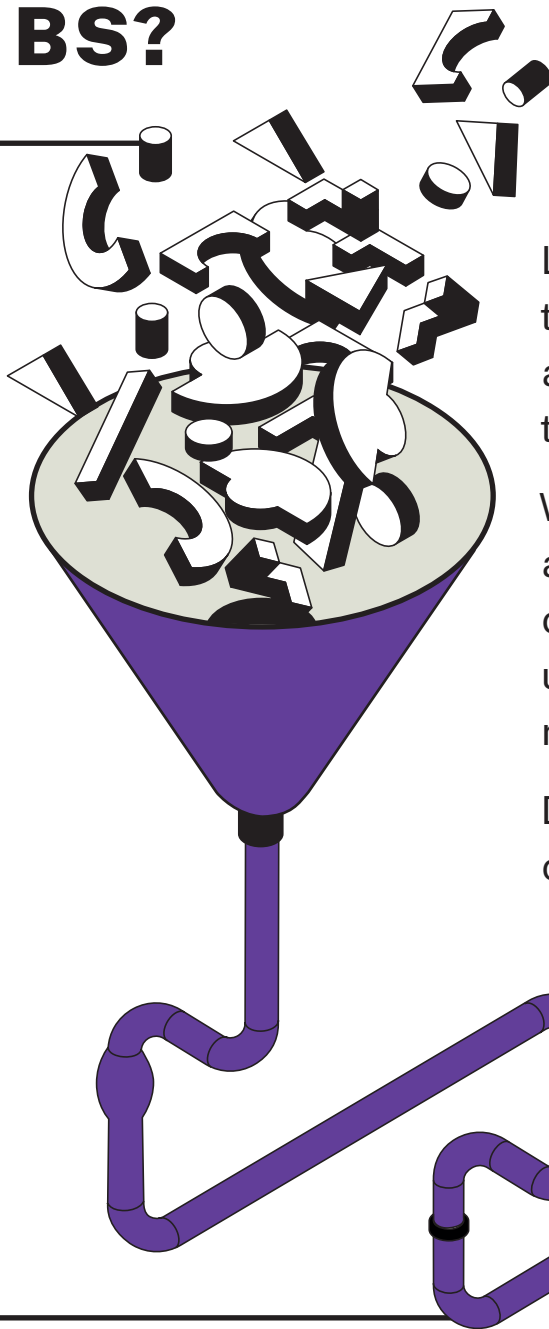
1 LLMs start by 'learning' single words.

2 By analysing other data related to that word, it can predict what should come next in the sentence.

EGG

CAT

WING

TWEET

PIGEON

BIRD

CHICK

NEST

WORM

After enough attempts and with enough data, LLMs can generate content that *sounds* human. Some experts say they aren't sure exactly how it works — one even said: "We just have no idea what any of it means."

LLMs also learn from what you tell them and what you type, to predict what you want to hear. This is what makes them seem like they have a 'personality'.

AI
OR BS?

LLMs have been fed so much data that they generate essays and ace exams. But they also present things as fact that aren't true.

While some experts believe LLMs are getting 'smarter' on their own, others say they're not actually understanding the words they repeat.

Do you really want to trust what a chatbot tells you?

An LLM is only as good as the 'diet' of data it's trained on. If that diet partly comes from the armpit of the internet, it could stink.

The most intelligent-sounding tool isn't necessarily all-knowing... It's just programmed to seem like it.