

Prosaic headaches around the AI chatbot megatrend and how they may evolve

Alexander C. Mueller

June 2023

Agenda

Goal: spotlight and contextualize data privacy challenges in AI

Review: Why are we talking about chat bots?!

- What is it? A big trend, a big model, a web form
- A poll of the room

Current events

- Banned here, banned there
- Notable issues

Business and machine learning

- Data, data, and data
- Expensive to train

What probably has to happen and its wrinkles...

Appendix: other ways to get in trouble...



Who is the speaker?

30 second resume:

- an ancient metro Saint Louis townie
- Ph.D. University of Michigan 2013 (math)
- a few years of data science
- founded privacy-enhancing tech company Capnion, Inc.

You might find it worthwhile to download the deck...

https://github.com/capnion/random/blob/master/acm_capnion_02june2023_tdwi.pdf

...to use these links to my Email, LinkedIn, or GitHub. I also recently started a local generative AI Meetup group.



GHOST PII

What is it? A chat bot

HA

In the fictional Battletech universe, how many ballistic weapon hardpoints does the Atlas battlemech have and what are their locations?



In the fictional Battletech universe, the Atlas battlemech is a massive and iconic assault-class 'mech. Typically, the Atlas has six ballistic weapon hardpoints distributed across its chassis. The locations of these hardpoints may vary depending on the specific variant of the Atlas, as different loadouts and configurations exist. However, a common configuration is as follows:



1. Right Arm: The Atlas usually has a single ballistic hardpoint in its right arm. This hardpoint allows for mounting a ballistic weapon such as an autocannon or gauss rifle.

© 1994-2001 Catalyst Game Labs Inc. The Atlas is a registered trademark of the BattleTech Alliance.

You can prompt “it” over the web and it will give cogent, reasonably well-written, and occasionally wildly incorrect answers to an extraordinarily broad variety of queries.



GHOST PII

What is it? A large piece of machine learning

A large language model (LLM) uses machine learning to model written discourse in the data used to train it.

Given a piece of input text, what should come next?

Basic example: ask it a question, it will give you an answer.

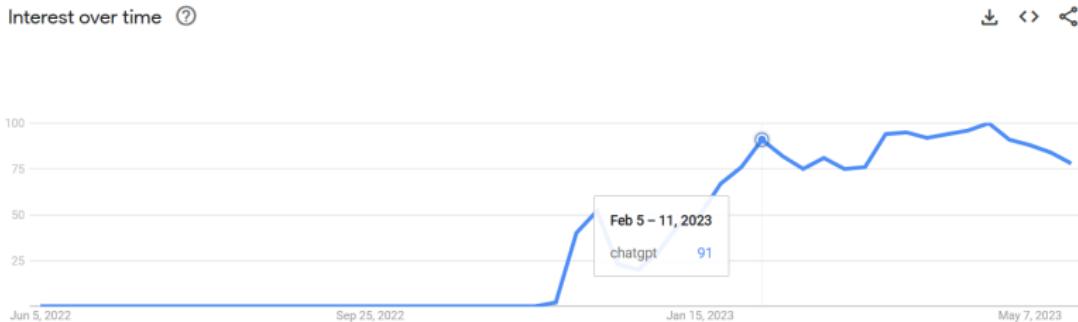
The training dataset is “large”- usually a big chunk of the internet with the porn and racism (hopefully) carefully excluded.

Famous and possibly familiar examples:

- OpenAI - ChatGPT, GPT-4, DALL-E 2
- Google - Bard
- GitHub - Copilot



A new hype cycle, love it or hate it...



I'm not here to sell you on this or that widget but rather...

- whatever “it” is, people are excited about it.
- it is going to come up at your office.
- opportunity and peril are definitely both in the mix.



Some basic polls

Feel free to say “yes” with discrete grumbling as appropriate...

Have you heard of generative AI, LLMs, and similar?

Have you used or experimented with any of these tools?

Do you use any of these tools at work...

- with your employer’s knowledge and permission?
- without any explicit oversight or permission?



Banned at Samsung

Samsung bans use of generative AI tools like ChatGPT after April internal data leak

Kate Park @kateparknews / 8:17 AM CDT • May 2, 2023

 Comment!



View the article via this [link](#).



GHST PII

Banned at Apple

Apple Bans Employees From Using ChatGPT Over AI Privacy Fears: WSJ

Tech giant Apple reportedly restricted internal use of the AI chatbot over data leak concerns, joining Samsung and other corporate giants.



By Jason Nelson

May 19, 2023

3 min read



View the article via this [link](#).



HOSTPII

What do they have in common?

New leak reveals the full Samsung Galaxy S23 lineup



PHONE



By Abhijeet Mishra

Last updated: February 2nd, 2023 at 10:45 UTC+01:00

View the article via this [link](#).



HOST PII

OpenAI's hot new Battletech sourcebook

HA

In the fictional Battletech universe, how many ballistic weapon hardpoints does the Atlas battlemech have and what are their locations?



In the fictional Battletech universe, the Atlas battlemech is a massive and iconic assault-class 'mech. Typically, the Atlas has six ballistic weapon hardpoints distributed across its chassis. The locations of these hardpoints may vary depending on the specific variant of the Atlas, as different loadouts and configurations exist. However, a common configuration is as follows:



1. Right Arm: The Atlas usually has a single ballistic hardpoint in its right arm. This hardpoint allows for mounting a ballistic weapon such as an autocannon or gauss rifle.

© 1994-2023 Catalyst Game Labs. The Atlas is a registered trademark of Catalyst Game Labs. All rights reserved.

ChatGPT is also a Battletech product and the Battletech people are not getting paid... Samsung is right to worry about helping someone create an industrial espionage product about them.



HOST PII

The IP lawsuit to watch

We've filed a lawsuit challenging GitHub Copilot, an AI product that relies on unprecedented open-source software piracy.

Because AI needs to be fair & ethical for everyone.

NOVEMBER 3, 2022

View the article via this [link](#).



HOST PPI

Regulatory issues

ChatGPT banned in Italy over privacy concerns

© 1 April



View the article via this [link](#).



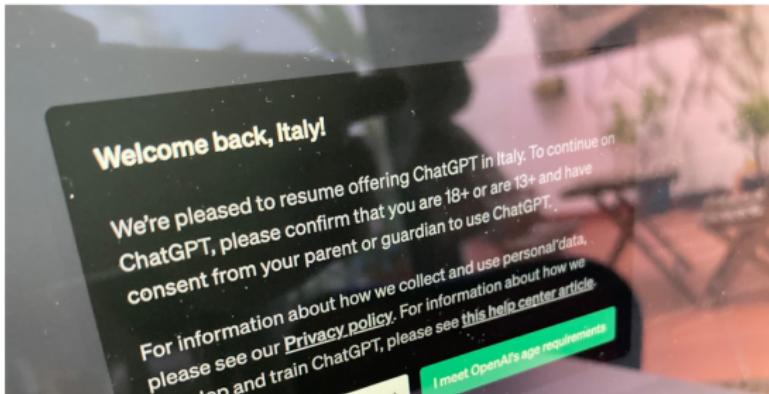
GHOS*T* PII

Regulatory turbulence

ChatGPT resumes service in Italy after adding privacy disclosures and controls

Natasha Lomas @riptari 1:57 PM CDT • April 28, 2023

 Comment



View the article via this [link](#).



HOSTPII

A new spin on an old problem

OpenAI confirms ChatGPT data breach

Some users payment information may have been visible to other users

 Add bookmark

Tags: OpenAI ChatGPT Chatbot AI Artificial Intelligence ML Machine Learning Data Breach
Data Leak Open Source Open Source Bug Bug Bounty



Olivia Powell
 05/03/2023



View the article via this [link](#).



HOST PII

Your LLM is currently subsidized



An analyst estimates that ChatGPT requires up to \$700,000 a day to run. Pavlo Gonchar/SOPA Images/LightRocket via Getty Images

“An analyst estimates that ChatGPT requires up to 700,000 dollars per day to run.” - read more [here](#)



GHOST PII

Data everyone wants

Microsoft threatens to restrict access to Bing's internet-search data to rival companies providing AI-powered online search tools

- Microsoft has told at least two licensee firms that using its Bing search index to feed their AI chat tools violates the terms of their contract
- Bing's search index – a map of the internet that can be quickly scanned in real time – is licensed by Microsoft to other firms that offer web search



Bloomberg

+ FOLLOW

Published: 11:10am, 25 Mar, 2023

Why you can trust SCMP



View the article via this [link](#).



GHOST PII

The hottest data of all...

... is the chat logs of megacorporate employees on the job.



They say if the product is free, then you are the product.
Everyday people put up with this, big corporations have good
reasons they are not going to.



Boring and probably unavoidable best practices...

The corporation needs a deal with (short list of options).

Exception with unique wrinkles: you are buying it from someone who is vaguely white-labeling inside another app.

The sticking point: **what can they do with your data?**

Your vendor will stay desperate to train on your chat logs.

The future of LLM is (ironically) probably to specialize by subject matter area, so you may be tempted to let them.

A model for you is great. A model about you is terrible. These may not be always easy to tell apart in a contract.

Right when you really get hooked on it, it will be suddenly be radically more expensive.



Questions and Conversation

Any questions?

acmueller@capnion.com

<https://www.linkedin.com/in/alexander-c-mueller-phd-0272a6108/>

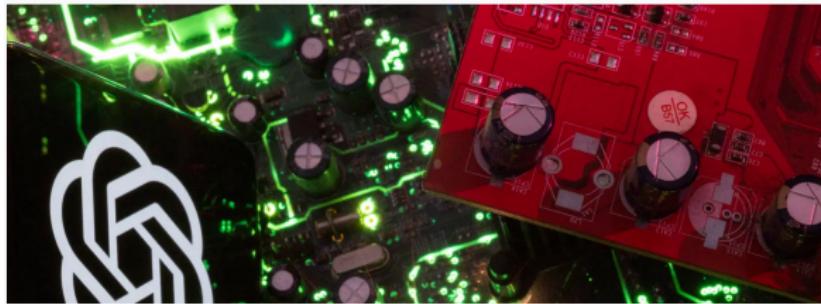
https://github.com/capnion/ghostpii_client

Appendix 1: Too desperate to answer...

MORONIC ROBOTIC

A US attorney faces punishment for citing fake cases ChatGPT fed him

The lawyer now regrets trusting the chatbot which misled him



View the article via this [link](#).



HOST PII

Appendix 1: Wrong in subtle ways...

6. Head: In some variations of the Atlas, a single ballistic hardpoint can be found in the head of the 'mech. This hardpoint is relatively small and can accommodate lighter ballistic weapons, such as a machine gun.

The more arcane the topic, the closer your LLM will get to being 100 percent wrong and still very confident about it.

LLMs are doing something more like memorization by rote and they don't know what they are saying. In this response, it confuses a technical meaning of "ballistic" internal to Battletech with the broader everyday, real-life meaning. All it knows is that it has seen "ballistic" in a sentence that looked like this one time somewhere...

