Less rules, more engineering with encrypted data-in-use

Alexander C. Mueller

July 2022

Agenda

Goal: awareness of future-proof new privacy technology

Trans-Atlantic data pipelines in need of future proofing and why

- (In-) Adequacy Frameworks
- Privacy Shield, etc. vs. Schrems I and II
- Notable EDPB Recommendations

Exciting new approaches

- Something for you to play with
- Qualitatively different encryption
- Some nomenclature
- Encrypted *data-in-use* and private pipelines

Who is the speaker?

30 second resume:

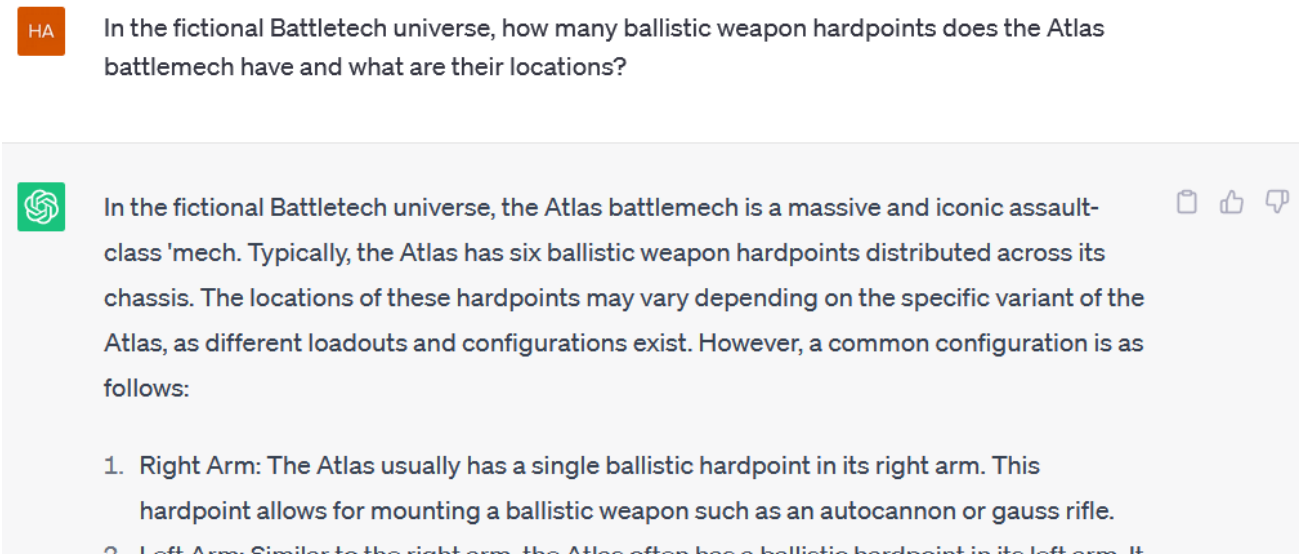
- an ancient metro Saint Louis townie
- Ph.D. University of Michigan 2013 (math)
- a few years of data science
- founded data privacy tech company Capnion, Inc.

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.

What is it? A chat bot



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 and complicated bit 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

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?

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.

GHOST PII

Very Current Events

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.

Very Current Events

New leak reveals the full Samsung Galaxy S23 lineup

PHONE By Abhijeet Mishra

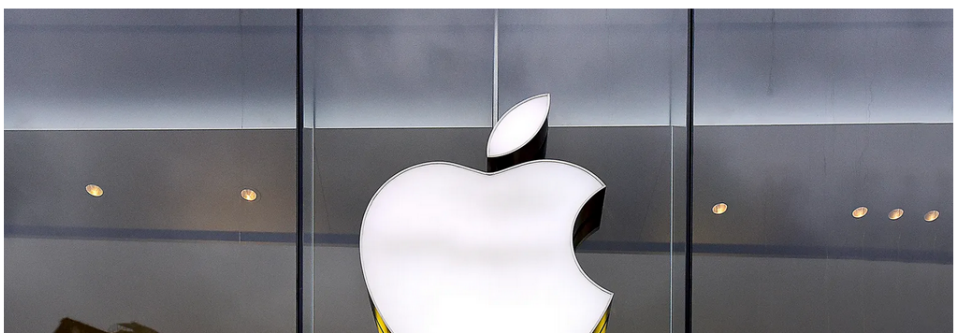
Last updated: February 2nd, 2023 at 10:45 UTC+01:00

View the article via this link.

Very Current Events

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.

Very Current Events

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 Bounty

Olivia Powell

05/03/2023

in 25

View the article via this link.

GHOST PII

Very Current Events

ChatGPT banned in Italy over privacy concerns

1 April

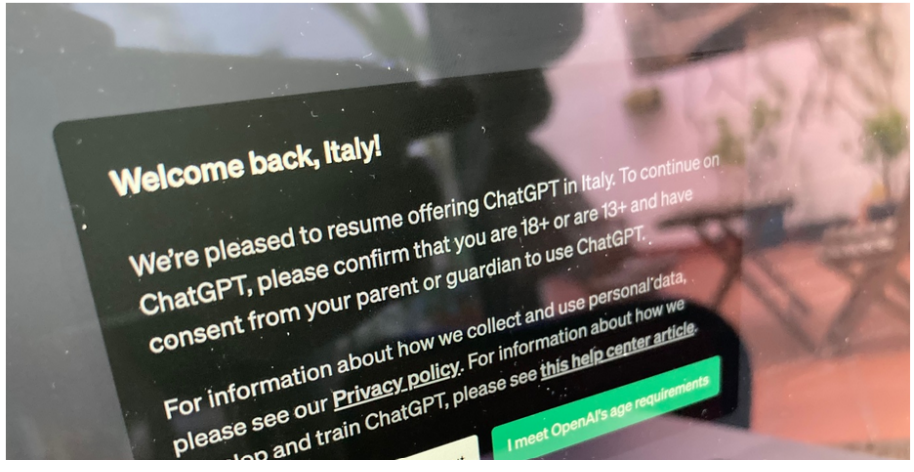
View the article via this link.

Very Current Events

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.

GHOST PII

Very Current Events

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.

Very Current Events

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

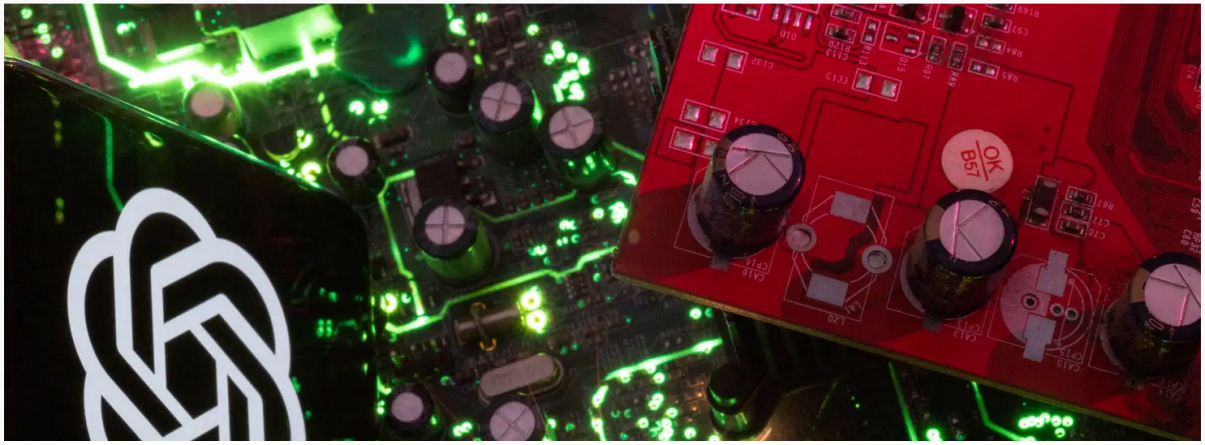
View the article via this link.

Very Current Events

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.

Very Current Events

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

View the article via this link.

Internal Tools

is this a good idea?

Questions and Conversation

Any questions?

acmueller@capnion.com

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

https://github.com/capnion/ghostpii_client

GHOST 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.

text