

AI IN 2024: TERMS TRENDS AND LLMS

A Guide to AI for Everyone

Alex Alcivar

This book is dedicated to Rubén

Table of Contents

Preface	3
Introduction	4
Computing and AI Models	7
Anatomy of an LLM	9
LLMs in 2023, LLMs in 2024	12
Strategies for Healthcare	15
AI for Healthcare: Then and Now	17
The New York Times Lawsuit	20
The New York Times describes ChatGPT	23
The Crux of the New York Times Lawsuit	27
OpenAI Responds to the New York Times	28
AI and Congressional Regulation	31
A Special Note for Teachers	36
What's Coming in 2024 and beyond	38
AI, War, and Terrorism	40
A Conclusion for Philosophers	41
Works Cited	43
About the Author	46

Preface

I was thinking about my 2023 in review, and how this year I sort of came back to computer science, and what about AI really ignited my passion.

There are many reasons to find Large Language Models, or LLMs, like chatGPT, captivating, but for me I think what I like so much is the helpfulness. It can be unwise to universalize, but I think we all find people can be less than forthcoming with their more useful secrets. Knowledge is power after all.

So after the initial shock of encountering an application that can speak so convincingly, the lasting impact for me is its constant unwavering dedication to being helpful. It's just math of course, but it becomes a human interaction that challenges us to see how often our own responses are constrained by priorities other than responsiveness.

I think LLMs represent a real dedication to open data and information, and I think that is actually one of the most disruptive things about them. LLMs will

give their best answer to anyone and do not ask you first "What is your background?" before deciding whether and how to answer your question.

I used to work on academic library software, and the most important thing that software does is check if the user is logged in, or using an on campus IP address, and only then provide access to all the online journal subscriptions for that educational institution. Despite the vast internet, knowledge was still very difficult to access. LLMs change that.

"How can I build a SAAS product with GenAI inside that will cut labor costs for large companies?" is a very important question, but so is "How can access to an LLM change a person's life?"

Introduction

For the last half of 2023, I attended as many AI related meetups in the Boston area as I possibly could. It had been a long time since I had dedicated myself to learning anything new related to computer science, but I, like many, was entranced by the speech capabilities of ChatGPT, and I wanted to

know more. By searching the internet I found one group, which led me to the next and the next, until I was running my own meetups for a global AI education startup, and then creating this, a guide to AI for everyone.

There are many guides to AI out there, and there will be many more written. Ironically, the safest space for writers looking to outcompete Large Language Models like ChatGPT might be to write about them. However, this book is not only about Large Language Models, but also about the various people affected by them and what I've seen happening in the last six months. This book is one picture, and one set of suggestions, but it does not aim to provide an exhaustive look at anything. Rather, the point is to provide a starting point, a window into the rapidly changing world of AI in 2024 and how we might start engaging with it.

The barrier of understanding between the average person and an AI developer is vast. I sit over here with an understanding I want to provide, but in

between are “What is a computer?”, “What is Machine Learning”, “What are statistics?”, “What is linear regression?”, “What is a file?”, “What is a GPU?”, “What is a Machine Learning Model?”, “What is Generative AI” and many other questions.

Those concepts are important, and this text will get to some of them, but I am going to try to write some things that are true about “Generative Artificial Intelligence”, or Gen AI, that don’t require that. Generative AI is AI that produces text, images, or video. To explain how it works, I would like to take a shortcut through the much more commonly understood concept of numbers:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
20 21 22 23 24 25 26 27 28 29 30 31 32 33 and so on
and so forth are numbers. I can write them down and use them later. I might do that for particularly special numbers that I’d like to remember. For example, I might write down the number for pi:

3.14159265359

Later I can use that number to do some math. Maybe I will calculate the area of a circle.

AI is, put simply, a very special, very cool, very big, series of numbers. We talk about AI Models, but that is just jargon for a copy of those numbers, a computer file just like a document but bigger than a movie file, full of row after row of numbers.

The point of this text is to facilitate understanding how that big file of numbers is created and why it can be used to create documents and images and eerily convincing chatbots to encourage consideration of how it will fit into the world and change the parameters of modern work.

Computing and AI Models

A proper introduction to computing involves a long theoretical discussion on the nature of problem solving. That is a fairly good place to start because the real thing that changed recently to allow for AI is a revolutionary computing algorithm, rather than a

revolutionary computer, though that did get built soon afterwards.

Computing, or computer science, is all about being given a problem and finding a solution. Every computer application is a series of small problems being solved on demand. You send an email, and a series of math problems are solved to produce an email on your colleague's phone. You press play on a video and a series of math problems are performed to fetch the video file from a server somewhere (a server is just another word for computer as far as we're concerned) and more math is performed to show you the movie on your phone.

This leads us to the basic entities of computer science: We have input numbers, we have a series of math calculations, and we have output numbers. You probably already know everything in a computer is numbers on some level, 0s and 1s, and that therefore means being a series of numbers is no defense against the claims of copyright infringement, or bad actions we will discuss in later chapters. This

muddies the waters quite a bit when considering copyright infringement, and that is why the way in which AI Models, those particular series of numbers, are created, and then the way in which they are used, is crucial.

Anatomy of an LLM

A Large Language Model is a computer program that is the product of a long series of calculations designed to find a set of numbers that optimally represent the structure of all human knowledge and language. When stated like that, it's unsurprising that it has captured the imagination and caused a frenzy of activity. Even the measured success of ChatGPT in that direction has fundamentally changed the nature of content creation and the assumptions that can be made about the source of an image, text, audio, or video.

This chapter seeks to describe the various components of an LLM more from a political perspective than a technical one, though

fundamentally the object being described is the same.

An LLM starts as a set of “training data”. This training data is things people have written, news articles, books, blog posts, coding forums, textbooks, literally any human produced text that contains words in an arrangement that you want to include in your Large Language Model.

Then you take a computer, and you run a lot of math on the training data. The computer creates a very large file filled with numbers. Each time the computer takes some of the copyrighted text, uses that text segment as input for a lot of math problems, and then updates the numbers in the file.

After a long time, and many many math problems, the computer has created a very large file full of numbers that represent the relationships between all the text ingested as best as possible.

This file has a very specific and special use. You can take this file of numbers, this LLM, and like putting a DVD in a DVD player, you can put it in an

LLM player, and spin it up. Then you can give it a prompt, a passage of text, and the LLM program will use the numbers in the LLM file to do a lot of math, and it will give you the most statistically likely next word. This is called “running inference”.

“But ChatGPT gives me a lot more than one word,” you might say. That’s true, and the way that happens is the LLM program does the math again, with its own predicted next word added to your prompt, and it finds the next word, and the next, and the next, until you tell it to stop. You can actually run inference on an LLM infinitely, and it will just continue to give you the next word like Netflix on autoplay.

Of course, like Netflix, commercially available LLMs like ChatGPT won’t give you infinite text. When we run an LLM like that on a computer and make it available on the internet, we call that a server, and the server costs money and it has limitations on how much math it can do every second.

Everything else about Large Language Models is changing rapidly, and frankly, this simplistic description is a sufficient, if not superior, starting point for examining the impacts and strategies of AI on things like healthcare, politics, and education.

LLMs in 2023, LLMs in 2024

LLMs in 2023 were very big. The model file, that magic series of numbers that can be used with the right math problems to generate text, that file was huge. It was too big and required too much math to run inference on these models using your average computer. For most of 2023, therefore, the way that everyone accessed AI was through special commercially available computing systems that had enough power to load these model files and run inference on them

Access to these commercial servers was provided through various online services, the most famous being chatGPT from OpenAI and Microsoft, and Bard from Google. This meant these companies

basically controlled the available AI chatbots for all but the most invested AI enthusiasts, people willing to put up the thousands of dollars required to build a computer capable of running an LLM.

Even for those enthusiasts, their options for running their own LLM were limited. For most of 2023 the GPT models from OpenAI and Microsoft were far superior to anything else available, and those model files, those sets of numbers, are secret. The most popular “open source” model, i.e. publicly available model file, was llama-2 from Meta, i.e. Facebook. By all standards, the llama-2 model is not as intelligent as the proprietary GPT models.

Things changed at the end of 2023 and the beginning of 2024. More open-source models were released, notably the Mistral and Mixtral models, and Hugging Face, a platform for sharing open-source models, took off. Computational strategies were popularized for making the model files smaller, particularly a method called “quantizing”. These quantized model files are small enough for your

average laptop or desktop computer to load and use to run inference, even without a GPU, i.e. a graphics card.

Another big difference between the LLMs available on the internet from Microsoft and Google in 2023, and these smaller LLMs that can be run on a personal computer, is that the LLMs available online are censored. They have guardrails and safety features built in to ensure that only appropriate content is discussed or produced by the chatbot. Each company has their own strategies for deciding what is appropriate, but generally they all erred on the side of caution, being willing to ban many topics: Legal advice, medical advice, explicit adult topics, strategies for violence, and offensive or impolitic humor.

Many of the newer open source models do not have any guardrails, and those that do can be modified by the AI community to create versions of them with the guardrails removed. With the advent of Hugging Face, an open source marketplace for

model files and ways to run them, the community has been engaged in a flurry of model merging, fine-tuning, retraining, and every type of permutation and combination that might gain attention or find a business use case.

Strategies for Healthcare

Generative AI Strategies for Healthcare are limited and difficult to justify. Generally people want their health care providers to be properly familiarized with their medical history without the assistance of AI. The discussion of AI in health care therefore tends to have more of a defensive tone. Frequently the justification for the use of Large Language models in medical settings is that it is improving on the sorry state of healthcare in many areas of the world even if it is not providing perfect recommendations.

In order to promote the use of AI, healthcare companies and their adjacent compatriots are highlighting the insufficiencies of medical systems in

the US to justify the use of AI to fill in the gaps. I have heard many examples in various product presentations. One appealed to the concept that doctors do not read the very long medical histories of some cancer patients, and therefore a summary of that history produced by an LLM would categorically be an improvement on the state of things, even if it did contain incorrect information or exclude crucial information.

Another example highlighted that a doctor on average has only 15 minutes for each patient, and that meant having suggested treatments and patient questions generated by AI would help a doctor who might otherwise be too tired or overworked to do their job properly. AI can also triage patient messages, the volume of which is increasing every day as more health centers ask their patients to use a text based message portal to communicate instead of phone calls. A Large Language Model can take a doctor's technical appointment followup note and use it to generate a patient friendly summary that the doctor can edit or approve.

Some of these uses are more comforting than others. Most people would not mind their doctor using AI to write nicer follow-up emails, but they also would not enjoy finding out their messages were being triaged by AI. What everyone will definitely not enjoy is if AI is used to ask health care providers to treat even more patients in a shorter time, rather than simply allowing them the relief of actually being able to provide better care.

The basic question can be characterized with the example of the 15 minute doctor: If they are given AI to increase their productivity, does the patient get 15 minutes of even more excellent care, or is the doctor told to handle one patient every ten minutes now that AI can handle so much of the paperwork?

AI for Healthcare: Then and Now

AI for healthcare until recently focused on very specialized models that could take an input like a brain scan and give an output like a percentage likelihood that scan had a brain bleed in it. Other models exist for other types of scans and diagnoses,

like cavities in teeth. I even saw a startup that claimed to be able to measure your brain health based only on how your finger interacts with your phone screen.

The dropoff of the use of these models is attributed to model drift, when the models become less accurate over time, or limited scope, since the models have to be trained for each task, but I suspect that in many cases the price simply wasn't justified. At those crucial moments of diagnosis, a health care provider has a lot of support for determining their course of action, and it is unlikely most AI diagnosis models increased provider outcomes or efficiency in some way to justify the cost of licensing such a system.

Large Language Models, however, have the potential of reducing administrative costs, and that could lead to the actual savings needed to justify the expenditure. They are also far less expensive to deploy and maintain than any specialized diagnostic model, and the variety of LLM providers means it is

safer for healthcare systems to become reliant to some degree upon them than specialized models created and maintained by a single company.

That is why use cases for LLMs in healthcare focus on things like insurance processing, patient appointments, and variable other quantifiable expenses related to provider services.

There are various legal issues to navigate with LLMs in healthcare, notably with HIPAA compliance, a fairly solvable problem, and with FDA classification and approval, a more difficult problem.

For HIPAA compliance, the issue mainly lies with the LLM vendor's guarantee to follow HIPAA guidelines when handling health information data. Some LLM providers already provide that HIPAA compliance guarantee, while others do not, a notable example of the latter being chatGPT.

For FDA approval, the main issue lies with the non-deterministic output of an LLM. What does that mean? It means basically that Large Language Models are a little random and inconsistent in their

results so no FDA trial can be done right now that would be able to accurately measure how an LLM would perform later on in a widespread clinical setting.

This is another reason administrative tasks are favored in health care. I suspect the vast majority of health care tasks will be to turn moments of creativity into moments of verification. The AI will generate the reports and the human will be there to verify and take responsibility for the outcome.

The New York Times Lawsuit

At the end of 2023, the New York Times sued OpenAI and Microsoft in Federal Court for copyright infringement and demanded money and the destruction of all the GPT models. I read the 70 page complaint filed by The New York Times against OpenAI and Microsoft and I do recommend reading it. If you do read it, here is some background on the context for the document.

The New York Times ("NYT") went to a nearby courthouse with this lawsuit describing why OpenAI

and Microsoft have violated civil laws regarding copyright, the evidence that they did this, and the solution they are proposing to fix the harm caused by this violation of law.

As people are fond of pointing out, anyone can file a civil lawsuit. You just go to the courthouse with a description of the grievance called a complaint.

From here OpenAI and Microsoft have a few moves:

1) They can file an Answer. This would be their own letter to the court, describing why the complaint is not legitimate. Typically the deadline to file an answer after receiving notice of a lawsuit in federal court is three weeks, but this can be extended with a Motion.

2) They can file a different kind of letter called a Motion. A motion is a letter to the court about a current case that is trying to change the parameters of the case. This would not address the substance of the complaint, i.e. the content, but might object to the procedure, like claiming the court does not have

jurisdiction or authority to handle this complaint and propose moving the case to another court or dismissing it.

Another motion they might file is a motion to sever the case into two cases, one between NYT and OpenAI and a separate one between NYT and Microsoft. They might also file a motion to extend the deadline for filing a response. You can file a motion for whatever you want, and the judge reads it and can have a hearing on the motion where both sides get to argue about it, and then the judge grants or denies the motion. Motions take up a lot of time in court cases.

3) OpenAI and Microsoft might prefer to say nothing at all, and the best avenue for that is for their lawyers to talk to the NYT lawyers and decide on a settlement, where they make a (usually) secret agreement and the NYT and OpenAI go to the court and ask the judge to let them do the settlement and dismiss the case.

However, if you read the 70 page letter the NYT filed, their complaint, it might seem like they are very upset, and would not want to settle. They are, after all, claiming billions of dollars in damages and demanding the destruction of all the OpenAI GPT models.

Two factors on that though:

- 1) A big part of claiming copyright is demonstrating a history of vociferously defending copyrighted works from unlicensed use.

- 2) Federal court is generally go big or go home.

A settlement is very possible, but what would be more exciting is a full court case. The NYT has requested a jury trial. If granted, the court will hear both sides and a jury will decide the outcome. The losing side can then try to appeal to the Supreme Court of the United States, to argue it again.

The New York Times describes ChatGPT

The first 22 pages of the NYT lawsuit describe the relationship between OpenAI and Microsoft.

How it started:

"Microsoft has invested at least \$13 billion in OpenAI Global LLC in exchange for which Microsoft will receive 75% of that company's profits until its investment is repaid, after which Microsoft will own a 49% stake in that company."¹

How it's going:

"Just three years after its founding, OpenAI shed its exclusively nonprofit status. It created OpenAI LP in March 2019, a for-profit company dedicated to conducting the lion's share of OpenAI's operations [...] The result: OpenAI today is a commercial enterprise valued as high as \$90 billion, with revenues projected to be over \$1 billion in 2024"²

"These commercial offerings have been immensely valuable for OpenAI. Over 80% of Fortune 500 companies are using ChatGPT. According to recent reports, OpenAI is generating

¹ [1 UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF NEW YORK THE NEW YORK TIMES COMPANY Civil Action](#) Accessed January 29 2024

² Ibid

revenues of \$80 million per month, and is on track to surpass over \$1 billion within the next 12 months."³

Three quotations are included from the CEO of Microsoft, Satya Nadella:

"But beneath what OpenAI is putting out as large models, remember, the heavy lifting was done by the [Microsoft] Azure team to build the computer infrastructure. Because these workloads are so different than anything that's come before. So we needed to completely rethink even the datacenter up to the infrastructure that first gave us even a shot to build the models. And now we're translating the models into products."⁴

"[W]e were very confident in our own ability. We have all the IP rights and all the capability. If OpenAI disappeared tomorrow, I don't want any customer of ours to be worried about it quite honestly, because we have all of the rights to continue the innovation. Not just to serve the product, but we can go and just do what we were

³ Ibid

⁴ Ibid

doing in partnership ourselves. We have the people, we have the compute, we have the data, we have everything."⁵

"And that gives us significant rights as I said. And also this thing, it's not hands off, right? We are in there. We are below them, above them, around them. We do the kernel optimizations, we build tools, we build the infrastructure. So that's why I think a lot of the industrial analysts are saying, 'Oh wow, it's really a joint project between Microsoft and OpenAI.' The reality is we are, as I said, very self-sufficient in all of this."⁶

There's also a succinct and impressive description of what it really takes to make ChatGPT:

"According to Microsoft, it operated as 'a single system with more than 285,000 CPU cores, 10,000 GPUs and 400 gigabits per second of network connectivity for each GPU server.' This system ranked in the top five most powerful publicly known supercomputing systems in the world."⁷

⁵ Ibid

⁶ Ibid

⁷ Ibid

In the picture painted by the NYT, it's kind of like Microsoft got to invest their money twice, once into OpenAI, and then also in their own AI Research and Development.

The Crux of the New York Times Lawsuit

The basic claim of the New York Times is that their articles, the entire body of work in the New York Times history, was crucial to the training process for the OpenAI GPT models, the LLMs that power chatGPT, and that Microsoft and OpenAI are using those models to compete with the New York Times and hurt their business. Both the unlicensed use of the New York Times articles and the business competition are important to the case in order to prove copyright infringement.

The examples provided in the lawsuit are of three general types:

- 1) Instances where chatGPT produced full text from New York Times articles with proper prompting

- 2) Instances where chatGPT or Bing used GPT models to read the latest New York Times articles and provide content or summary, thereby diverting traffic from the New York Times Website
- 3) Evidence that the New York Times training data was weighted with particular importance in the GPT training process and is the main reason for its success.

OpenAI Responds to the New York Times

OpenAI responded soon after the New York Times filed their lawsuit, but they did so in a blog post rather than in court. Their response starts with a succinct summary of their position:

“Our position can be summed up in these four points, which we flesh out below:

We collaborate with news organizations and are creating new opportunities

Training is fair use, but we provide an opt-out because it's the right thing to do

‘Regurgitation’ is a rare bug that we are working to drive to zero

The New York Times is not telling the full story”⁸

OpenAI appears to be leaning into the idea that their use of New York Times data is transformative use, an exception under copyright law. They would claim that all the mathematical analysis to create the Large Language Model and the process by which the output is generated are by their nature transformative processes that provide a categorical copyright exception. They do not address the commercial competition in their blog post, and it is not a coincidence the New York Times highlighted that so much. It is possible they are drawing on a recent Supreme Court precedent.

The recent Andy Warhol Supreme Court case might signify a changing interpretation of fair use

⁸ [OpenAI and journalism](#) Accessed January 24 2024

that takes into account whether the transformative work is competing in the same market as the original one.

Justice Sotomayor delivers the Court's opinion in that case, *Andy Warhol Foundation For The Visual Arts, Inc. v. Goldsmith Et Al*, and at one point states: "In this case, however, Goldsmith's original photograph of Prince, and AWF's copying use of that photograph in an image licensed to a special edition magazine devoted to Prince, share substantially the same purpose, and the use is of a commercial nature"⁹

To me, the implication presented is that fair use of copyrighted materials can be impacted by whether the result is competing in the same commercial marketplace. The New York Times lawsuit therefore highlights the way that GPT models and their outputs compete directly with directly accessing the New York Times as a customer without Bing, or chatGPT, as an intermediary.

⁹ [21-869 Andy Warhol Foundation for Visual Arts, Inc. v. Goldsmith \(05/18/2023\)](#) Accessed January 20, 2024

AI and Congressional Regulation

Events at the end of January 2024 related to AI generated fake images have led to increased demand for AI regulation, which means one particular bipartisan AI regulation bill from the U.S. Senate is getting more attention.

The press release for the bill states:

“U.S. Senators Brian Schatz (D-Hawai‘i) and John Kennedy (R-La.) introduced bipartisan legislation to provide more transparency on content generated by artificial intelligence (AI). The new bill would help ensure people know when they are viewing AI-made content or interacting with an AI chatbot by requiring clear labels and disclosures.”¹⁰

I have a few immediate questions:

- 1) Would this even help with the issues at hand?
- 2) Would this violate the first amendment to the Constitution of the United States?

¹⁰ [Schatz, Kennedy Introduce Bipartisan Legislation To Provide More Transparency On AI-Generated Content](#) accessed Jan 19, 2024

3) Which kind of math counts as regulated AI generated content?

The press release goes on to say:

“‘People deserve to know whether or not the videos, photos, and content they see and read online is real or not,’ said Senator Schatz.”¹¹

I am sympathetic to this idea, but I am not sure it would survive a US Supreme Court challenge. That is probably why the rest of the press release tries to conflate people being fooled and scammed:

“‘AI is moving quickly, and so are the companies that are developing it. Our bill would set an AI-based standard to protect U.S. consumers by telling them whether what they’re reading, seeing or hearing is the product of AI, and that’s clarity that people desperately need,” said Senator Kennedy.

[...]

“The Schatz-Kennedy AI Labeling Act would:

¹¹ Ibid

“Require that developers of generative AI systems include a clear and conspicuous disclosure identifying AI-generated content and AI chatbots;

“Make developers and third-party licensees take reasonable steps to prevent systematic publication of content without disclosures; and

“Establish a working group to create non-binding technical standards so that social media platforms can automatically identify AI-generated content.”¹²

Consumer protection laws enforced by the Federal Trade Commission like this proposed bill rely on the financial harm perpetrated by deceptive advertising. I think there's not much basis to necessarily connect AI generated content with deceptive advertising. AI generated content can easily provide good information to consumers regardless of whether it is labeled that way.

Then there is the question of "what is AI generated content?"

¹² Ibid

The bill itself says "GENERATIVE ARTIFICIAL INTELLIGENCE SYSTEM.—The term “generative artificial intelligence system” means any system that uses artificial intelligence (as defined in section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019) to generate or substantially modify image, video, audio, multimedia, or text content."¹³

I tracked down that section and here it is:

"(g) ARTIFICIAL INTELLIGENCE DEFINED.—In this section, the term “artificial intelligence” includes the following:

(1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.

(2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception,

¹³ [Download File: AI Labeling Act of 2023 | U.S. Senator Brian Schatz](#) accessed Jan 29 2024

cognition, planning, learning, communication, or physical action.

(3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks.

(4) A set of techniques, including machine learning, that is designed to approximate a cognitive task.

(5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting."¹⁴

This proposed bill to regulate AI is citing a definition from a fiscal year end document from 2019. That definition is extremely broad and more than a little vague. It seems that we can do better when it comes to AI regulation, and if legislators don't handle the line between consumer protection

¹⁴ [John S. McCain National Defense Authorization Act for Fiscal Year 2019](#) Accessed January 29 2024

and free speech, the judiciary will have to do it for them.

A Special Note for Teachers

There are no tools out there that can reliably inform you if something was written using AI or not. The transformative power of AI means that very quickly the tools to generate essays assigned for homework will far outpace the ability of tools to detect them. I can easily imagine tools specifically designed to imitate a student's particular writing style and introduce convincing errors and mistakes.

I can see two strategies to deal with a world in which a student can generate an essay in two minutes. The first is to simply increase their workload. Instead of one essay, assign five essays. Assign an essay on a different topic every single night. This brings us to the second strategy, which is oral assessments. Have them give an oral presentation on their essay to other students.

It is quite possible that with these strategies, students would learn much faster anyway. Ironically,

the use for which LLMs are most effective is self-learning. An LLM is unparalleled in helpfulness, tirelessness, and tolerance when it comes to teaching. It is worrisome that so many teachers are discouraging their use under the guise of maintaining academic honesty. This is like discouraging your students from learning how to drive because of environmental issues.

I hear from many students that they are discouraged from using generative AI, and they admit to doing so with tinges of shame in their demeanor. Meanwhile, they will graduate to a world in which every professional will have been pushed to increase their productivity with LLMs. If AI is not embraced by traditional educational institutions, new institutions that do emphasize using AI will arise to replace them. This is because AI skills will become some of the most valuable skills in the workforce, and those who use AI effectively will succeed faster.

What's Coming in 2024 and beyond

All of these factors are combining together to slow the adoption of large centralized closed LLMs like GPT, and push the adoption of smaller open source LLMs, or fully licensed proprietary LLMs for particular use cases or companies. Many large companies are building their own internal LLM system to assist their staff in order to maintain data privacy while still gaining the benefits of an AI powered workforce.

Fully licensed proprietary LLMs provide the legal security and the privacy that some companies need. Many companies do not want to send their data to OpenAI, and they also want to be sure they are legally covered against all copyright issues.

Open source models provide the low cost, flexibility, and control that other companies need. They don't, however, necessarily provide protection against copyright issues depending on how the model was trained and how the regulation and court cases shake out over time.

Open source models continue to become more diverse and powerful. Some are large, and some are small enough to run on a personal computer, and fairly soon, a phone.

2024 also brings us a United States Presidential election, which is a period of heightened media activity and content production. I expect AI will play a central role in this election year as the various political stakeholders involved in the campaigns realize that AI has the power to energize the populace in a way that few other topics do these days.

There is also a strong potential for the proliferation of LLMs specifically tailored to political causes, like a “voteGPT” that is a chatbot that encourages the users to go vote. On a more manipulative level, one might find an LLM based chatbot that advocates persuasively for a particular candidate.

I would also be remiss if I did not mention the ease with which misinformation can be spread by AI.

Misinformation can be obvious, like a false news story, or it can be less detectable. For example, generative AI can be used to automate online comments on political forums or social networks that make it seem like a large and diverse group of people support a particular viewpoint from various perspectives. Many people form impressions of general sentiments based on the various anonymous opinions they see in their online content.

AI, War, and Terrorism

The line between war and terrorism can be blurry and arbitrary. AI has the potential to make it blurrier. This is because AI is the automation of attention, and attention is the key to political violence. Generally until now in order to tailor destruction to the advantage of a particular belief system or viewpoint, human attention and emotion was required to sustain the shaping of violence.

That is a fairly abstract introduction, so let's zoom in on the LLM. Large Language Models transform their inputs into output. You can give it an

instruction like “Generate code to attack a server on the internet, send me all the data, and destroy all the data on that server”. That server might belong to a hospital. Right now chatGPT and other online tools won’t generate that code for you, but with the rise in open source LLMs, and the general drive of technology, AI could do so in the future.

The line between terrorism and war in fact crystallizes quite quickly. Who is given AI with destruction powers? If it is only the government, then AI will mostly be used for war. If it is open source, and everyone has access to powerful AI in the future that can create and execute malicious code, then we might have a proliferation of online terrorism as a small group’s whims can be amplified by AI systems that can automate political attention and violence.

A Conclusion for Philosophers

Up until now I have not mentioned AGI, Artificial General Intelligence, which is basically the fancy word for a computer that is actually as smart as a human. Really it is the worrisome concept that AI

will advance to the point of consciousness, and self-consciousness, at which point we will have even more of an ethical conundrum.

Unfortunately, there does not seem to be any way that even an advanced AI could be proven to be conscious, sentient, human, feel pain, or whatever quality might elevate it to personhood. In fact, as AI more effectively emulates humanity, the more we will have to question what it is that makes us human. Perhaps it is simply the way we come into existence for no good reason, fail to achieve our goals, and die pointlessly.

It might be possible that in creating AI in our own image, we disillusion ourselves of our own humanity, reifying instead the existence of machines. There are many in the AI community who are also interested in longevity, and aspire to immortality, digitization of their consciousness, further immersion in virtual realities, and generally a desire to become more like the machine.

As a society, we will have to deal with the way that AI challenges how we define ourselves and others as human. It is possible that society will experience various upheavals as more and more advanced AI is created, embodied, and given agency to perform tasks.

Works Cited

“Download File: AI Labeling Act of 2023 | U.S.”

Senator Brian Schatz,

<https://www.schatz.senate.gov/download/ai-labeling-act-of-2023> . Accessed 29 January 2024.

“John S. McCain National Defense Authorization

Act for Fiscal Year 2019.” *John S. McCain*

National Defense Authorization Act for Fiscal

Year 2019,

<https://www.congress.gov/115/bills/hr5515/BILLS-115-hr5515-enr.pdf> . Accessed 29 January 2024.

“OpenAI and journalism.” *OpenAI*, 8 January 2024, <https://openai.com/blog/openai-and-journalism> . Accessed 29 January 2024.

“Schatz, Kennedy Introduce Bipartisan Legislation To Provide More Transparency On AI-Generated Content” *Senator Brian Schatz*, 24 October 2023, <https://www.schatz.senate.gov/news/press-releases/schatz-kennedy-introduce-bipartisan-legislation-to-provide-more-transparency-on-ai-generated-content> . Accessed 29 January 2024.

Sotomayor, Sonia. “21-869 Andy Warhol Foundation for Visual Arts, Inc. v. Goldsmith (05/18/2023).”

Supreme Court, 18 May 2023,

https://www.supremecourt.gov/opinions/22pdf/21-869_87ad.pdf . Accessed 29 January 2024.

“UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF NEW YORK THE

NEW YORK TIMES COMPANY Civil

Action.” *The New York Times*, 6 December

2023,

https://nytco-assets.nytimes.com/2023/12/NYT_Complaint_Dec2023.pdf . Accessed 29 January

2024.

About the Author

Alex Alcivar lives just north of Boston with his husband. He received a Bachelor of Arts in Computer Science and Political Science from Grinnell College in 2012. You can reach him with any questions, comments, or corrections at TermsTrendsLLMs@gmail.com