GPT: Revolutionizing Monitoring and Logging Systems

Clay Langston

4.23.2023

What is an LLM?

‘Large Language Model’

Generates likely strings in the same grammar, that follow an input string

Not magic

LLM Providers

	Advantages
OpenAI	The market leader, offers the most sophisticated models available today
Bard AI	Google integration
stability.ai	Open source, can be run on your own infrastructure – Good from a privacy perspective

LLMs are Liars (sometimes)

Likely strings do not mean ‘accurate’ strings

Best suited to workflows with human review

Better prompts = better results

Single Shot Prompt

make a list of characters from Dune, in the format of first letter of first letter of first name, and full last name concatenated together as a single string

PaulAtreides
DuncanIdaho
Stilgar
GurneyHalleck
LetoAtreides
AliaAtreides
FeydRautha
JessicaAtreides
BaronVladimirHarkonnen
GaiusHelenMohiam
WensiciaCorrino

Few Shot Prompt

make a list of characters from Dune, in the format of first letter of first letter of first name, and full last name concatenated together as a single string

example:
Paul Atredies = patreides
Duncan Idaho = didaho

Leto Atreides = latreides
Gurney Halleck = ghalleck
Jessica Atreides = jatreides
Baron Vladimir Harkonnen = bvharkonnen
Stilgar = stilgar
Thufir Hawat = thawat
Feyd-Rautha Harkonnen = frharkonnen
Gaius Helen Mohiam = ghmohiam
Wensicia Corrino = wcorrino

Tuning

A tuned model can be thought of as ‘many shot’

Ability to train on more examples than can fit in a prompt

Higher quality results

```
{"prompt": "<prompt text>", "completion": "<ideal generated text>"}
{"prompt": "<prompt text>", "completion": "<ideal generated text>"}
{"prompt": "<prompt text>", "completion": "<ideal generated text>"}
```

Building Extractions

Extract each seperate field from this log file:

{\"Level\":4,\"callerIpAddress\":\"[CENSORED]\",\"category\":\"AuditLogs\"
account\",\"operationVersion\":\"1.0\",\"properties\":{\"activityDateTime\":\"
account\",\"additionalDetails\":[],\"category\":\"UserManagement\",\"correl
[CENSORED]\",\"id\":\"Directory_[CENSORED]_9XW55_232870592\",\"initia
[CENSORED]\",\"roles\":[],\"userPrincipalName\":\"patredies@birch5.io\"}},\
Directory\",\"operationType\":\"Update\",\"result\":\"success\",\"resultReasc
[CENSORED]\",\"modifiedProperties\":[{\"displayName\":\"AccountEnabled
Properties\",\"newValue\":\"\\\"AccountEnabled\\\"\",\"oldValue\":null}],\"ty
urceId\":\"/tenants/[CENSORED]/providers/Microsoft.aadiam\",\"resultSign

Example:
Level: 4
category: Audit Logs
operationVersion: 1.0
activityDateTime: 2023-04-17T15:04:02.4797521+00:00
activityDisplayName: Disable account
category: UserManagement
correlationId: [CENSORED]
initiatedBy: {\"user\":{\"displayName\":null,\"id\":\"[CENSORED]\",\"ipAddre
loggedByService: Core Directory
operationType: Update
result: success

Write regexes that extract each of those field values:

Level: \d+
category: Audit\sLogs
operationVersion: \d+\.\d+
activityDateTime: \d{4}-\d{2}-\d{2}T\d{2}:\d{2}:\d{2}\.\d+\+\d{2}:\d{2}
activityDisplayName: [\w\s]+

Summarization

"original": "{\"Level\":4,\"callerIpAddress\":\"[CENSORED]\",\"category\":\"AuditLogs\",\"correlationId\":\"[CENSORED]\",\"durationMs\":0,\"operationName\":\"Disable account\",\"operationVersion\":\"1.0\",\"properties\":{\"activityDateTime\":\"2023-04-17T15:04:02.4797521+00:00\",\"activityDisplayName\":\"Disable account\",\"additionalDetails\":[],\"category\":\"UserManagement\",\"correlationId\":\"[CENSORED]\",\"id\":\"Directory_[CENSORED]_9XW55_232870592\",\"initiatedBy\":{\"user\":{\"displayName\":null,\"id\":\"[CENSORED]\",\"ipAddress\":\"[CENSORED]\",\"roles\":[],\"userPrincipalName\":\"patredies@birch5.io\"}},\"loggedByService\":\"Core Directory\",\"operationType\":\"Update\",\"result\":\"success\",\"resultReason\":\"\",\"targetResources\":[{\"administrativeUnits\":[],\"displayName\":null,\"id\":\"[CENSORED]\",\"modifiedProperties\":[{\"displayName\":\"AccountEnabled\",\"newValue\":\"[false]\",\"oldValue\":\"[true]\"},{\"displayName\":\"Included Updated Properties\",\"newValue\":\"\\\"AccountEnabled\\\"\",\"oldValue\":null}],\"type\":\"User\",\"userPrincipalName\":\"bharkkonnen@birch5.io\"}],\"userAgent\":null},\"resourceId\":\"/tenants/[CENSORED]/providers/Microsoft.aadiam\",\"resultSignature\":\"None\",\"tenantId\":\"[CENSORED]\",\"time\":\"2023-04-17T15:04:02.4797521Z\"}"

Summarization

an account was disabled in the Core Directory service of the Microsoft.aadiam provider on April 17, 2023 at 3:04 pm. The account was disabled by a user with the user principal name patredies@birch5.io, and the target user was bharkkonnen@birch5.io. The result of the operation was successful.

Building a Plugin

Starting Template:

https://github.com/elastic/template-kibana-plugin/

Helpful guide:
https://dilshankelsen.com/how-to-create-a-plugin-for-kibana/

```
plugins/
└── sg_kibana_demo_plugin
    ├── README.md
    ├── common
    │   └── index.ts
    ├── kibana.json
    ├── package.json
    ├── public
    │   ├── application.tsx
    │   ├── components
    │   │   └── app.tsx
    │   ├── index.scss
    │   ├── index.ts
    │   ├── plugin.ts
    │   └── types.ts
    ├── server
    │   ├── index.ts
    │   ├── plugin.ts
    │   ├── routes
    │   │   └── index.ts
    │   └── types.ts
    ├── target
    │   └── public
    │       ├── sgKibanaDemoPlugin.chunk.0.js
    │       ├── sgKibanaDemoPlugin.chunk.0.js.map
    │       ├── sgKibanaDemoPlugin.plugin.js
    │       └── sgKibanaDemoPlugin.plugin.js.map
    ├── translations
    │   └── ja-JP.json
    └── tsconfig.json
```

Summarizer Example

Table JSON

Search field names

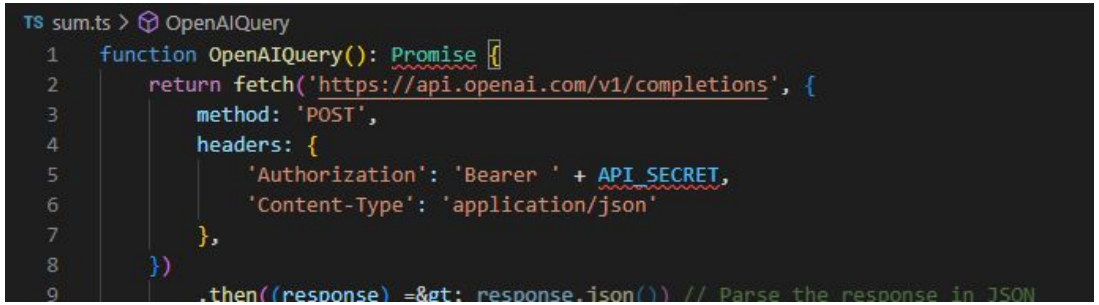
Actions	Field	Value
	t original	{"Level":4,"callerIpAddress":"[CENSORED]","category":"AuditLogs","correlationId":"[CENSORED]","durationMs":0,"operationName":"Disable account","operationVersion":"1.0","properties":{"activityDateTime":"2023-04-17T15:04:02.4797521+00:00","activityDisplayName":"Disable account","additionalDetails":[],"category":"UserManagement","correlationId":"[CENSORED]","id":"Directory_[CENSORED]_9X
	GPT Description	an account was disabled in the Core Directory service of the Microsoft.aadiam provider on April 17, 2023 at 3:04 pm. The account was disabled by a user with the user principal name patredies@birch5.io, and the target user was bharkkonnen@birch5.io. The result of the operation was successful.

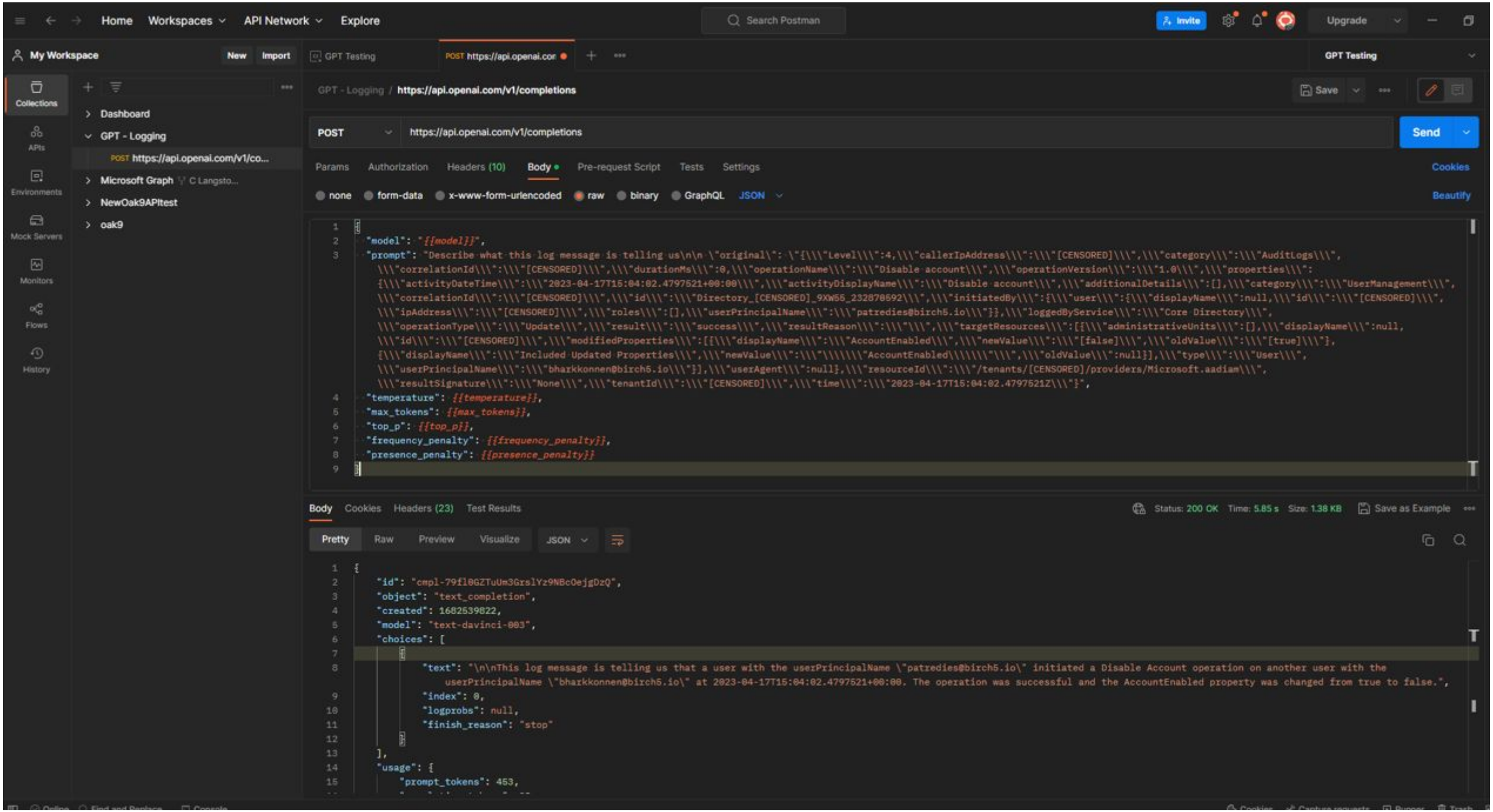
Cont'd

Token limit means we can only pass limited data

Raw event may not fit – Trim to what is necessary

Raw event may contain information you do not want to send – Find and replace sensitive data




Home
Workspaces
API Network
Explore
Search Postman
Invite
Upgrade
My Workspace
New
Import
GPT Testing
POST https://api.openai.com/v1/completions
Collections
APIs
Environments
Mock Servers
Monitors
Flows
History
Dashboard
GPT - Logging
POST https://api.openai.com/v1/co...
Microsoft Graph
NewOak9APItest
oak9
GPT - Logging / https://api.openai.com/v1/completions
Save
POST
https://api.openai.com/v1/completions
Send
Params
Authorization
Headers (10)
Body
Pre-request Script
Tests
Settings
Cookies
none
form-data
x-www-form-urlencoded
raw
binary
GraphQL
JSON
Beautify
{
"model": "{{model}}",
"prompt": "Describe what this log message is telling us\n\n \"original\": \"{\\\"Level\\\":4,\\\"callerIpAddress\\\":\\\"[CENSORED]\\\",\\\"category\\\":\\\"AuditLogs\\\",
\\\"correlationId\\\":\\\"[CENSORED]\\\",\\\"durationMs\\\":0,\\\"operationName\\\":\\\"Disable account\\\",\\\"operationVersion\\\":\\\"1.0\\\",\\\"properties\\\":
{\\\"activityDateTime\\\":\\\"2023-04-17T15:04:02.4797521+00:00\\\",\\\"activityDisplayName\\\":\\\"Disable account\\\",\\\"additionalDetails\\\":[],\\\"category\\\":\\\"UserManagement\\\",
\\\"correlationId\\\":\\\"[CENSORED]\\\",\\\"id\\\":\\\"Directory_[CENSORED]_9XW55_232870592\\\",\\\"initiatedBy\\\":{\\\"user\\\":{\\\"displayName\\\":null,\\\"id\\\":\\\"[CENSORED]\\\",
\\\"ipAddress\\\":\\\"[CENSORED]\\\",\\\"roles\\\":[],\\\"userPrincipalName\\\":\\\"patredies@birch5.io\\\"}},\\\"loggedByService\\\":\\\"Core Directory\\\",
\\\"operationType\\\":\\\"Update\\\",\\\"result\\\":\\\"success\\\",\\\"resultReason\\\":\\\"\\\",\\\"targetResources\\\":[{\\\"administrativeUnits\\\":[],\\\"displayName\\\":null,
\\\"id\\\":\\\"[CENSORED]\\\",\\\"modifiedProperties\\\":[{\\\"displayName\\\":\\\"AccountEnabled\\\",\\\"newValue\\\":\\\"[false]\\\",\\\"oldValue\\\":\\\"[true]\\\"},
{\\\"displayName\\\":\\\"Included Updated Properties\\\",\\\"newValue\\\":\\\"\\\\\\\\\\\"AccountEnabled\\\\\\\\\\\"\\\",\\\"oldValue\\\":null}],\\\"type\\\":\\\"User\\\",
\\\"userPrincipalName\\\":\\\"bharkkonnen@birch5.io\\\"}],\\\"userAgent\\\":null},\\\"resourceId\\\":\\\"/tenants/[CENSORED]/providers/Microsoft.aadiam\\\",
\\\"resultSignature\\\":\\\"None\\\",\\\"tenantId\\\":\\\"[CENSORED]\\\",\\\"time\\\":\\\"2023-04-17T15:04:02.4797521Z\\\"}",
"temperature": {{temperature}},
"max_tokens": {{max_tokens}},
"top_p": {{top_p}},
"frequency_penalty": {{frequency_penalty}},
"presence_penalty": {{presence_penalty}}
}
Body
Cookies
Headers (23)
Test Results
Status: 200 OK
Time: 5.85 s
Size: 1.38 KB
Save as Example
Pretty
Raw
Preview
Visualize
JSON
{
"id": "cmpl-79fl0GZTuUm3GrslYz9NBcOejgDzQ",
"object": "text_completion",
"created": 1682539822,
"model": "text-davinci-003",
"choices": [
{
"text": "\n\nThis log message is telling us that a user with the userPrincipalName \"patredies@birch5.io\" initiated a Disable Account operation on another user with the
userPrincipalName \"bharkkonnen@birch5.io\" at 2023-04-17T15:04:02.4797521+00:00. The operation was successful and the AccountEnabled property was changed from true to false.",
"index": 0,
"logprobs": null,
"finish_reason": "stop"
}
],
"usage": {
"prompt_tokens": 453,

OpenAI Params

Temperature

Tokens

Top P

Frequency Penalty

Presence Penalty

Model

Variable	Type	Initial value
open_api_key	secret	••••••••••••••••••••••••••••••••
temperature	default	0.7
max_tokens	default	256
top_p	default	1
frequency_penalty	default	0
presence_penalty	default	0
model	default	text-davinci-003

OpenAI Models

LATEST MODEL	DESCRIPTION	MAX TOKENS
`gpt-4`	More capable than any GPT-3.5 model, able to do more complex tasks, and optimized for chat.'	8,192 tokens
`gpt-4-32k`	Same capabilities as the base gpt-4 mode but with 4x the context length.	32,768 tokens
`gpt-3.5-turbo`	Most capable GPT-3.5 model and optimized for chat at 1/10th the cost of text-davinci-003	4,096 tokens
`text-davinci-003`	Can do any language task with better quality, longer output, and consistent instruction-following than the curie, babbage, or ada models.	4,097 tokens
`code-davinci-002`	Optimized for code-completion tasks	8,001 tokens

Privacy and Confidentiality Considerations

OpenAI does not use content sent to them via the API for training new models

They *do not* say they do not retain logs or other properties

Sending sensitive data is always a risk

3. Content

(a) **Your Content**. You may provide input to the Services ("Input"), and receive output generated and returned by the Services based on the Input ("Output"). Input and Output are collectively "Content." As between the parties and to the extent permitted by applicable law, you own all Input. Subject to your compliance with these Terms, OpenAI hereby assigns to you all its right, title and interest in and to Output. This means you can use Content for any purpose, including commercial purposes such as sale or publication, if you comply with these Terms. OpenAI may use Content to provide and maintain the Services, comply with applicable law, and enforce our policies. You are responsible for Content, including for ensuring that it does not violate any applicable law or these Terms.

(b) **Similarity of Content**. Due to the nature of machine learning, Output may not be unique across users and the Services may generate the same or similar output for OpenAI or a third party. For example, you may provide input to a model such as "What color is the sky?" and receive output such as "The sky is blue." Other users may also ask similar questions and receive the same response. Responses that are requested by and generated for other users are not considered your Content.

(c) **Use of Content to Improve Services**. We do not use Content that you provide to or receive from our API ("API Content") to develop or improve our Services. We may use Content from Services other than our API ("Non-API Content") to help develop and improve our Services. You can read more here about how Non-API Content may be used to improve model performance. If you do not want your Non-API Content used to improve Services, you can opt out by filling out this form. Please note that in some cases this may limit the ability of our Services to better address your specific use case.

Contact Info

Name:

Clay Langston

Email:

clangston@oak9.io