# ****PET Instance 1: PrivateGPT****

## **Task 1 - Description**

**Name of PET Instance -** PrivateGPT  
**Website -** <https://chat.private-ai.com/>

### **Function and Utilities**

PrivateGPT is a Privacy-Preserving web-based application that acts as an intermediary between users and powerful generative AI models (such as ChatGPT and Cohere). It mainly automatically identifies, redactions, and masks personally identifiable information (PII), protected health information (PHI), and payment card information (PCI) in text and documents prior to sending any data to cloud-based AI services. This makes it privacy regulation (GDPR, CPRA, HIPAA) compliant and limits the possibility of sensitive information leakage in cases where AI-powered chatbots or language models are used.

### **Why I Chose This PET**

I selected PrivateGPT since it provides a real-world, practical demonstration of how privacy technology may be applied with well-liked AI tools. With organizations and individuals Continually using AI to gain productivity and automation, there is a risk of privacy. PrivateGPT shows the way to reduce these risks and make the AI technology usage safe and responsible. Its simplicity, transparency and well documented interface make it usable by a beginner as well as an advanced user who cares about privacy.

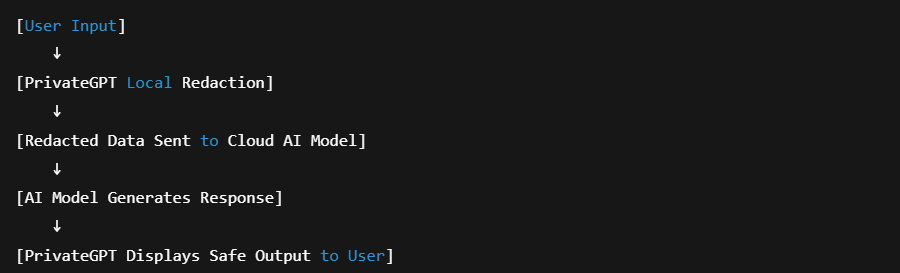


Figure 1 - PrivateGPT acts as a privacy filter between the user and the AI model, redacting sensitive data before sending it to the cloud.

## **Task 2 - Hands-On Exploration**

### **Step 1 - Access and Account Creation**

* Navigated to the [PrivateGPT website](https://chat.private-ai.com/).
* Developed a new account at no cost with personal email address.
* Once my email was verified, I logged in and it redirected me to the dashboard.

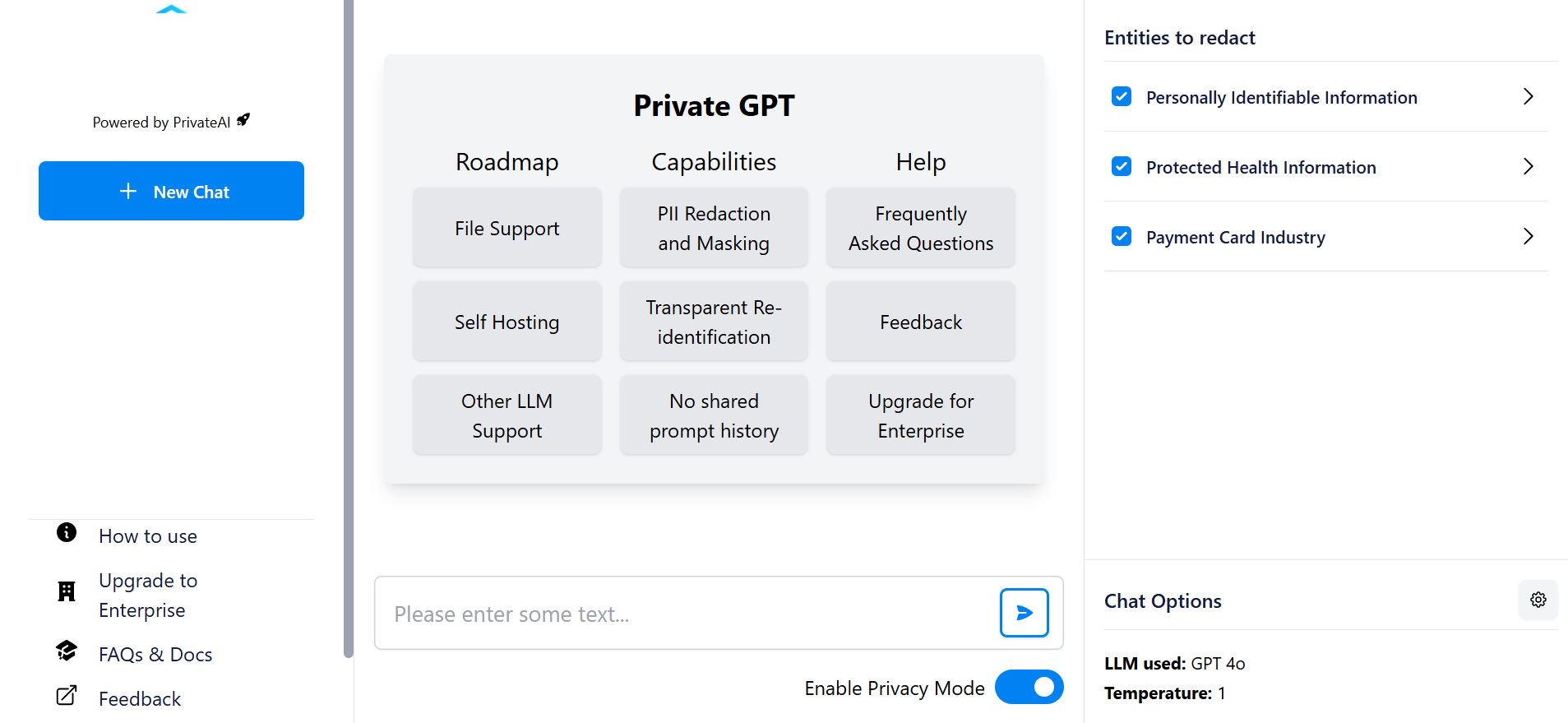


Figure 2 - PrivateGPT login and main dashboard interface.

### **Step 2 - Exploring Features and Settings**

* Hovered over the gear icon labeled “Settings” to see privacy options.
* On the dashboard, one could select the type of the redaction: PII, PHI, and PCI.
* It was possible to select alternative AI models, such as GPT-3.5 Turbo, GPT-4 and Cohere.
* Scanned FAQ and docs sections.

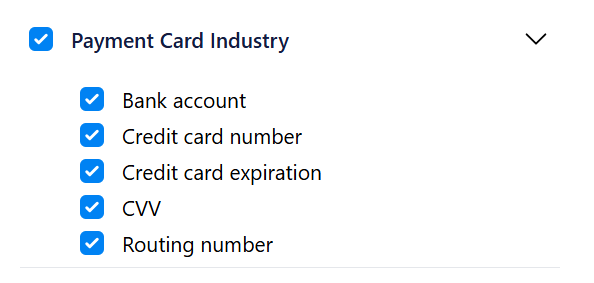
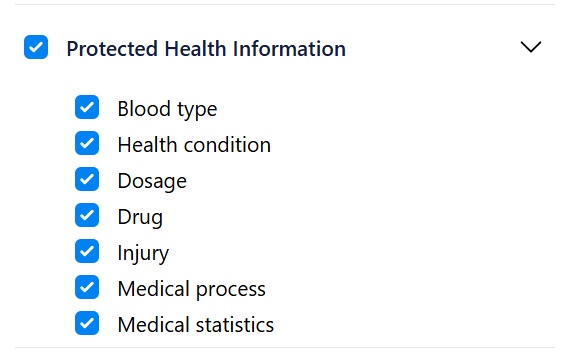
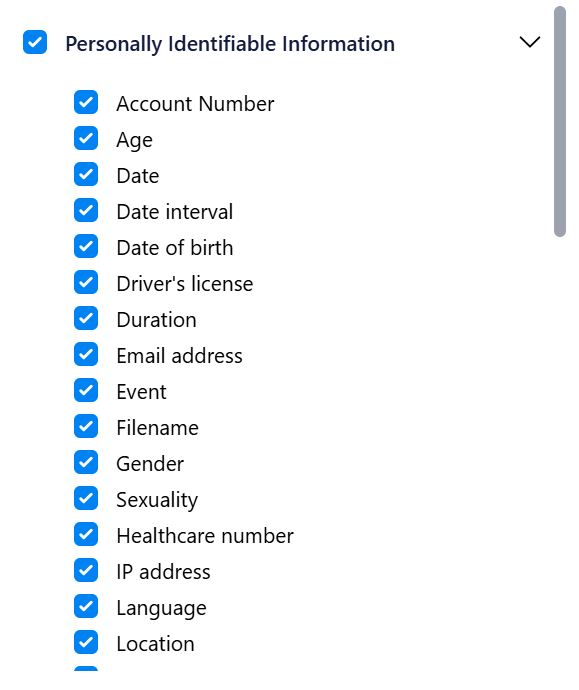
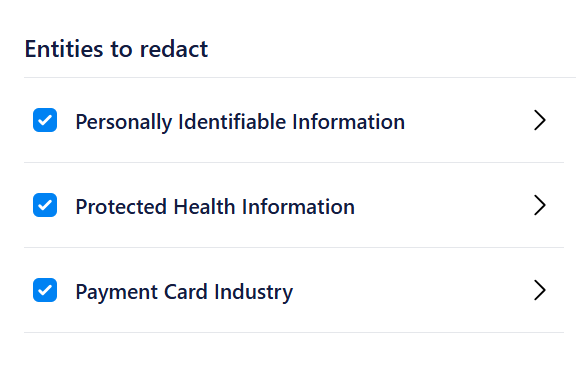
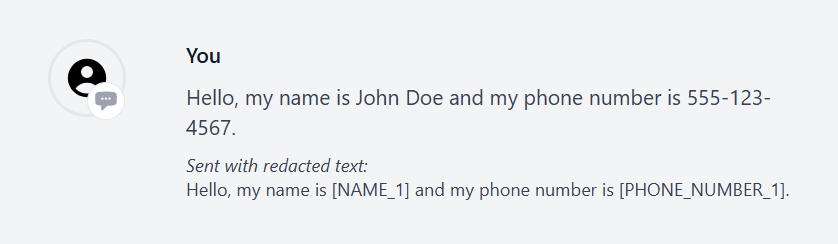


Figure 3 - Privacy controls and redaction options in PrivateGPT

### **Step 3 - Testing Text Redaction**

* The text of a sample prompt with fake personal information was typed in the chat window:
* “Hello, I am John Doe and my phone number is 555-123-4567“.
* PrivateGPT automatically replaced or masked the sensitive information prior to processing it after the message was sent.
* The chat log presented the redacted version.

****

### **Figure 4 -** Redaction in Action

### **Step 4: Document Redaction**

* Press the button “Upload Document” and provided the sample Word document with fake personal information (e.g. CV with name, address, email, etc.).
* The document was run through PrivateGPT and the version with all personal information removed was provided back.

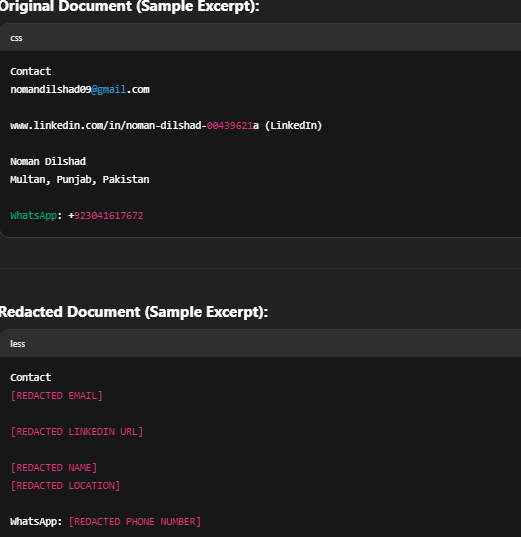


Figure 5 - Document redaction: original and redacted versions compared

### **Step 5: Experimenting with Redaction Controls**

* Redaction behavior on various kinds of data by toggling privacy settings (on/off).
* As an illustration, disabled PCI redaction and sent a message containing a fake credit card number; the redaction was not performed, which proved that the settings were working.

### **Step 6: Observations and Reflections**

* Tool is easy to use, no technical knowledge needed.
* Redaction was performed in real-time on chat and documents.
* Masking of all sensitive data was done successfully.
* Documentation was logical and useful.

## **Issues/Challenges**

* Free account is limited in its use.
* Redaction of files was most effective with conventional formats.
* In rare cases, the more-complex or less-common PII formats may not be identified.

## **What I Learned**

A good example of a privacy-enhancing technology that is both usable and secure is PrivateGPT. It demonstrates that users can retain firm control of their sensitive information even in the cases where they utilize cloud-based AI. The practical procedure emphasized the relevance of checking the privacy settings, and how using automated tools can contribute to attaining compliance with data protection standard.

# ****PET Instance 2: Anonymous Camera****

## **Task 1: Description**

**Name:** Anonymous Camera  
**Link:** <https://apps.apple.com/us/app/anonymous-camera/id1504102584>  
**Function and Features:**  
Anonymous Camera is an iOS mobile app designed to provide real-time privacy protection when capturing photos and videos. The main features include:

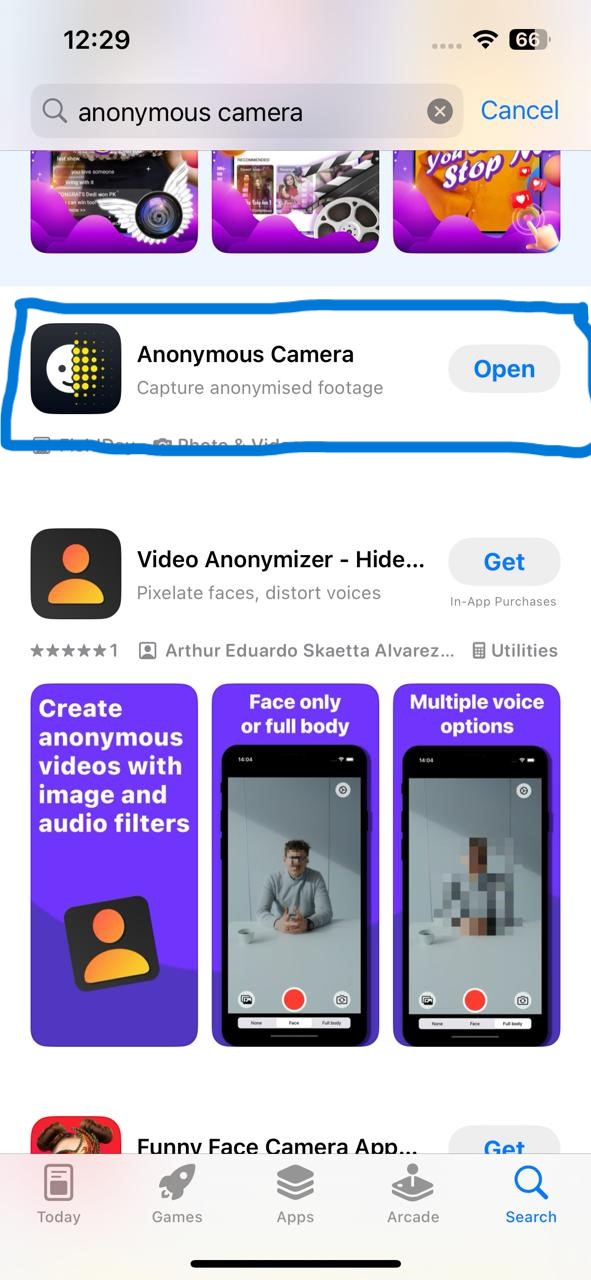
* Real-time blurring or masking of faces and bodies in both photos and videos.
* Ability to remove metadata (such as location, date, and device info) from captured media.
* Audio distortion for anonymizing voices in video recordings.
* No account or login required, ensuring minimal personal data is retained.
* All processing is done locally on the device nothing is sent to any external servers.
* Easy-to-use toggles for enabling/disabling privacy features before or after capture.

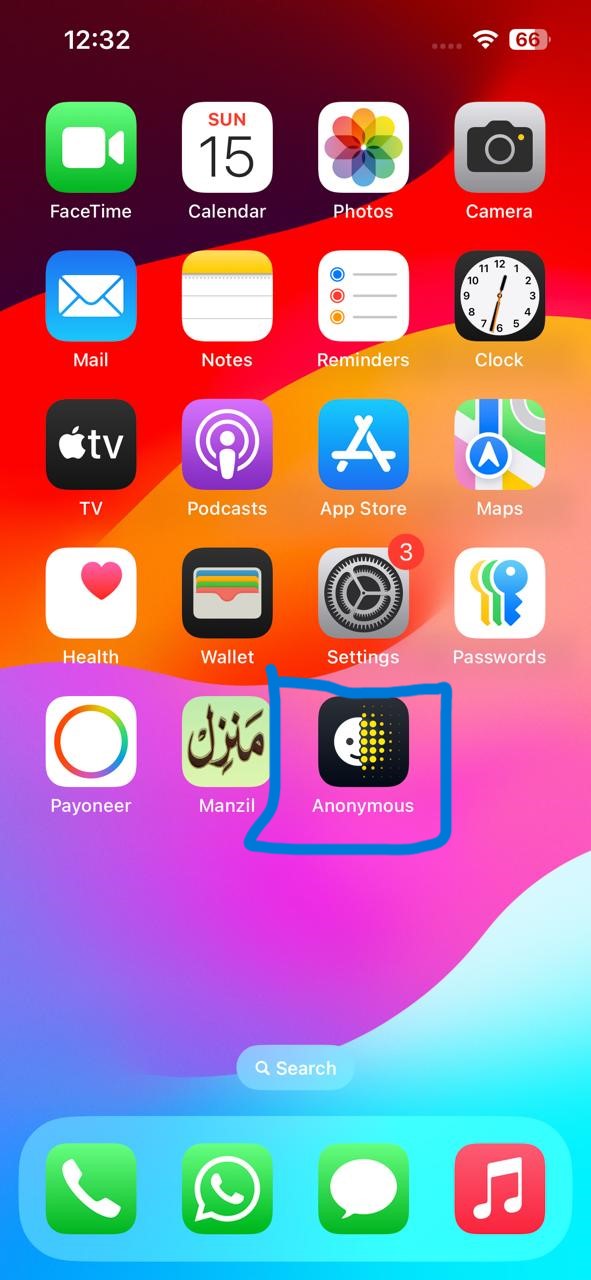
## **Why I Chose It**

Anonymous Camera demonstrates how privacy-enhancing technology can be applied beyond just data by anonymizing visual media at the moment it is created. This is invaluable for journalists, researchers, activists, or anyone who needs to document sensitive situations while protecting the identities of those involved. Its real-time processing and strong privacy-first design make it a practical and trustworthy tool.

## **Task 2: Hands-On/Exploration**

### **How I Set It Up:**

1. Searched for “Anonymous Camera” in the Apple App Store and installed the application on an iPhone.  
   ****
2. Opened the app, which immediately launched the camera interface without requiring registration or login.

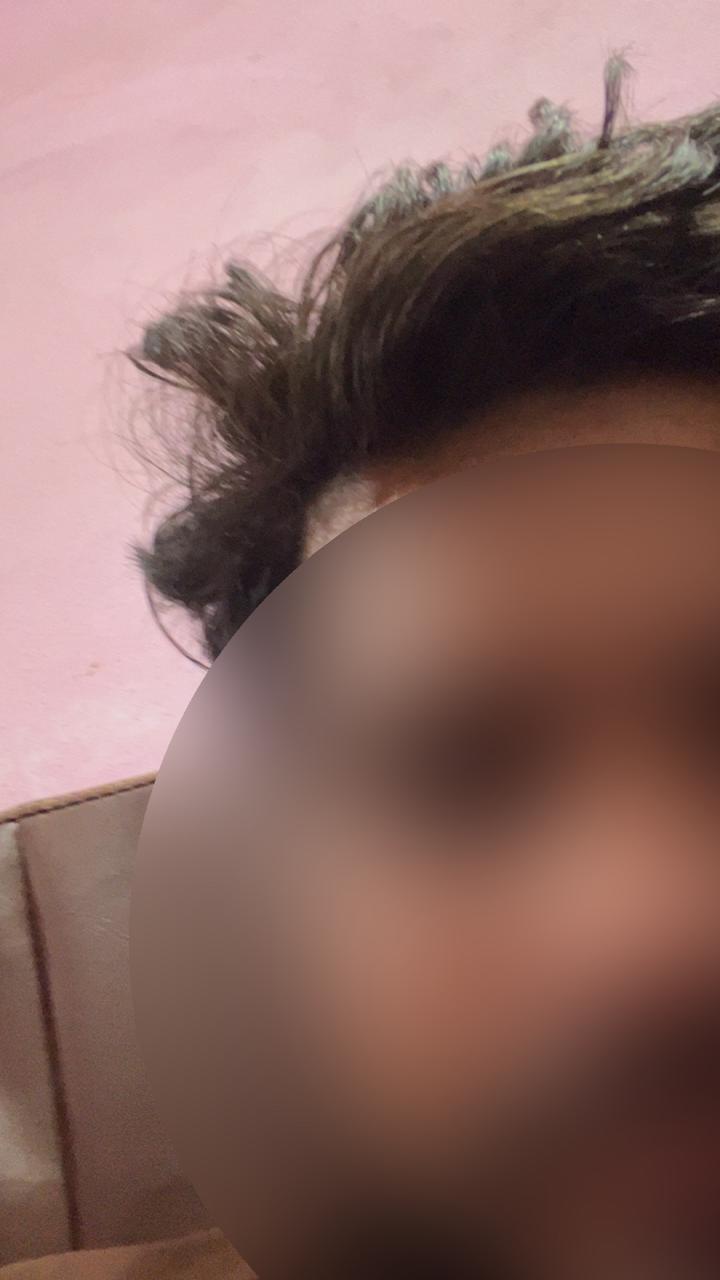


1. Granted the necessary permissions for camera and microphone access as prompted by iOS.



### **What I Did:**

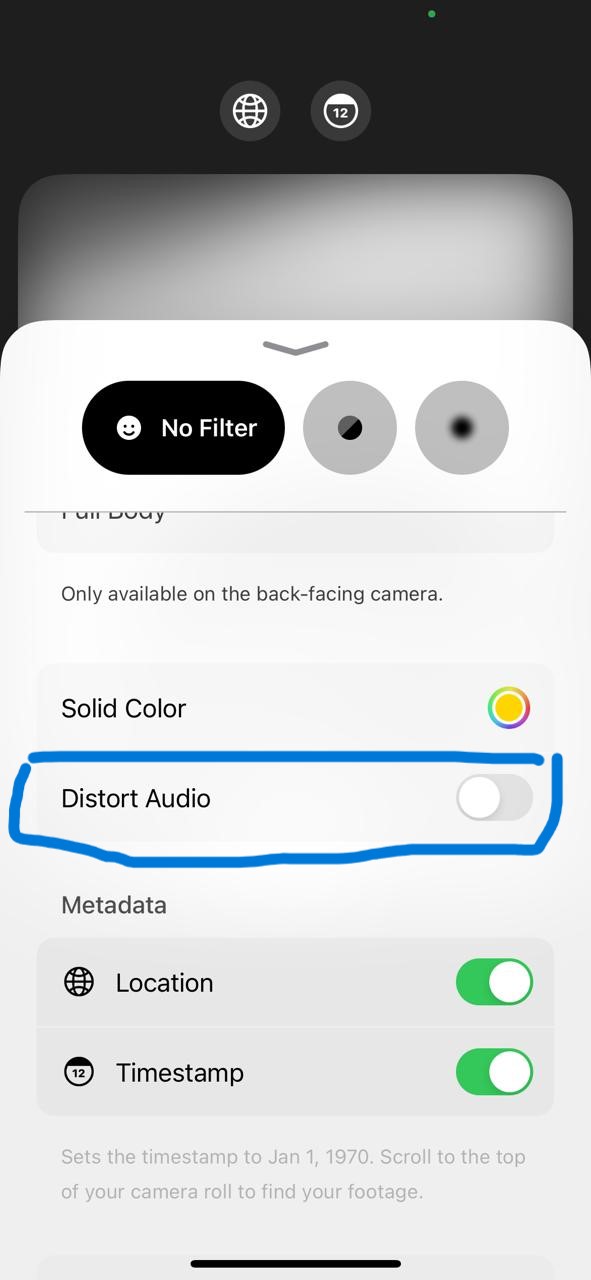
* Explored all the on-screen privacy controls:
  + Enabled real-time face blurring, which automatically blurred all detected faces in the camera view.

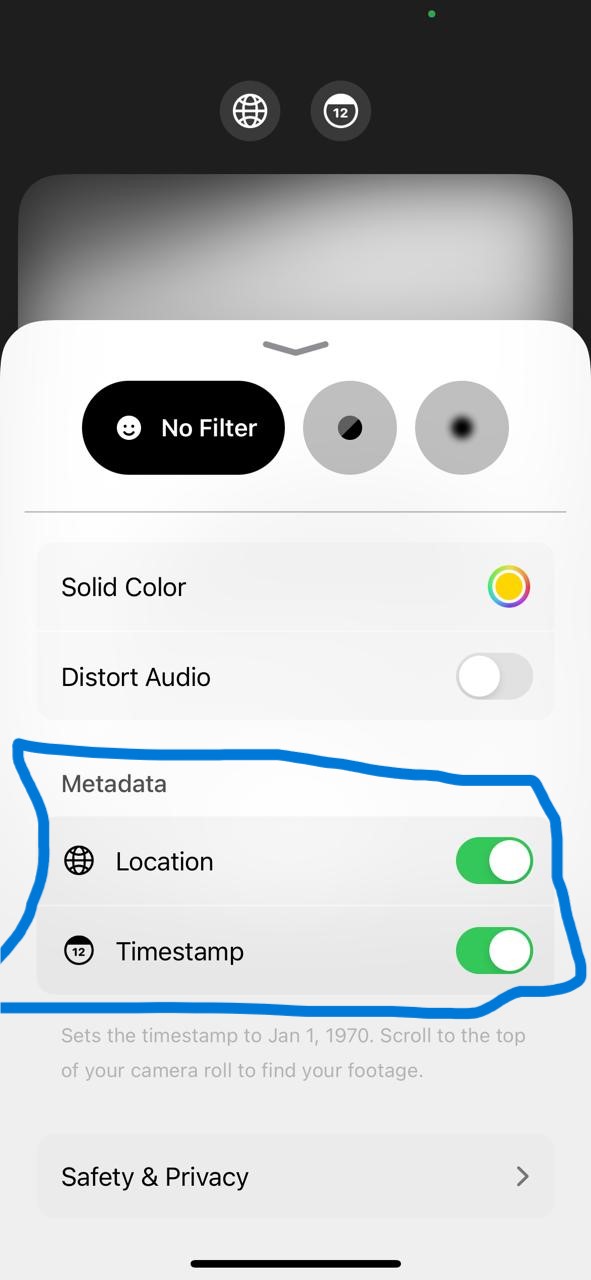


* + Enabled full-body masking for maximum anonymity.



* + Enabled audio distortion to anonymize voices when recording video.



* Saved anonymized photos and videos to the device.
* Verified that no identifying metadata (e.g., GPS or device info) remained by examining the saved files in the device’s photo gallery and using a metadata viewer.  
  
* Attempted to undo or reverse the blurring/masking with photo editing tools—unsuccessfully, confirming the effectiveness of the privacy filters.

### **Observations & Learnings**

* The app is extremely intuitive; privacy features are clear, and toggles are easy to access.
* Real-time blurring and masking work efficiently, even with multiple people in the frame or with people moving.
* All processing is handled locally on the phone, so no sensitive data leaves the device.
* Metadata removal and audio distortion features work as promised.
* The app does not collect or store any personal information about users.
* Limitation: only available for iOS devices, and certain advanced features may not work on older iPhones.

### **Personal Reflection**

Anonymous Camera is a practical, highly effective privacy-enhancing technology that makes visual anonymity accessible and easy. Its real-time, on-device processing ensures that sensitive media can be safely created and shared without risking personal privacy. The simple interface and robust privacy guarantees make it a valuable tool for anyone who needs to capture sensitive moments or protect others’ identities.

# ****PET Instance 3: Onerep****

## **Task 1: Description**

**Name:** Onerep  
**Link:** <https://onerep.com/>  
**Function and Features:**  
Onerep is an online privacy tool designed to help users locate and remove their personal information from hundreds of data broker websites. These sites collect and publish personal data such as names, addresses, phone numbers, and more, often making this information available for anyone to find online. Onerep’s main features include:

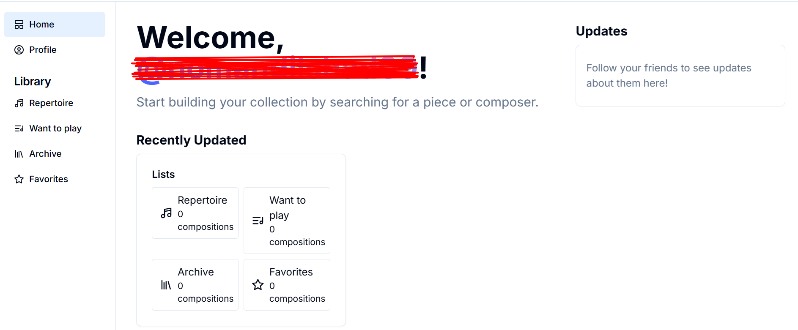
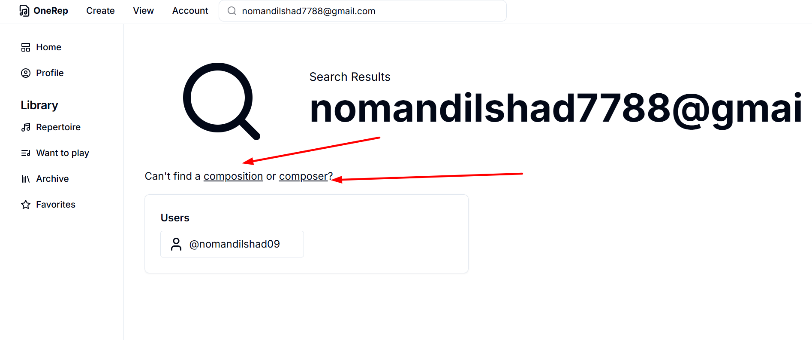
* Automated scans across 190+ data broker sites for exposed personal information.
* Detailed dashboard showing where your data is found and removal progress.
* Automated removal requests to brokers on your behalf, in line with privacy laws like GDPR and CCPA.
* Ongoing monitoring with periodic rescans to keep your data private.
* Helpful resources and customer support for managing your online privacy.

### **Why I Chose It:**

Onerep stands out as a PET because it addresses a widespread real-world privacy problem: unwanted online exposure of personal data. Many people are unaware of how many data brokers hold their information, and manual removal is time-consuming and confusing. Onerep’s automated, easy-to-use system empowers individuals to regain control over their digital footprint and proactively defend their privacy.

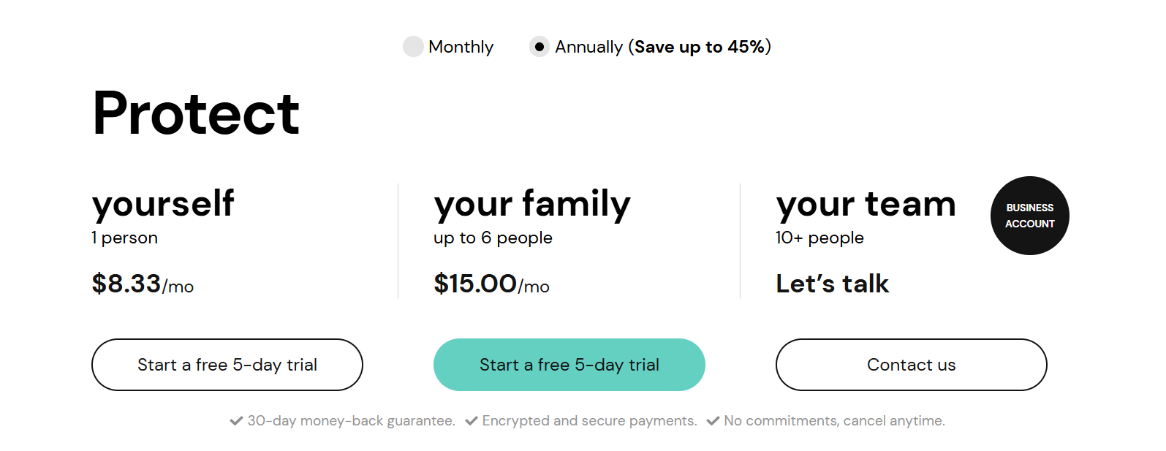
## **Task 2: Hands-On/Exploration**

### **How I Set It Up:**

1. Navigated to the Onerep website (<https://onerep.com/>).  
   
2. Entered a sample full name and city/state to begin a scan for personal data exposure.  
   
3. Provided an email address (required for results and dashboard access).
4. Received scan results displaying the number of broker sites where personal information was found.
5. Explored the dashboard, which allows users to see removal status and progress.

### **What I Did**

* Clicked through the dashboard to view detailed reports from different broker sites.
* Examined the “removal in progress” status updates for different sites.
* Attempted to add additional information to see if more results were found.
* Explored the free trial option, which requests payment details but offers limited-time access to automated removals.



* Monitored updates in the dashboard as removal requests were submitted to data brokers.

### **Observations & Learnings**

* The interface is simple and user-friendly, making it easy to track data exposure and removal efforts.
* Onerep found dozens of records on various people search sites after just one scan.
* Manual removal from these sites would be extremely time-consuming; Onerep’s automated approach saves significant effort.
* Some broker sites responded quickly, updating status within days, while others took longer.
* The service is subscription-based (with a free trial), and full automation is only available to paid users.
* Privacy is clearly prioritized no data is sold, and removal requests are handled securely.

## **Personal Reflection**

Onerep is a valuable privacy-enhancing tool for anyone concerned about their personal information circulating online. Its automated scanning and removal system makes digital privacy management practical for everyday users. Although it is a paid service, the time saved and peace of mind provided make it worthwhile, especially for those frequently targeted by spam, robocalls, or identity theft.

# ****PET Instance 4: Web Browser Privacy Test****

## **Task 1: Description**

**Name:** Web Browser Privacy Test  
**Link:** <https://webbrowsertools.com/privacy-test/>  
**Function and Features:**  
The Web Browser Privacy Test is a free, browser-based tool designed to help users quickly assess the privacy and security posture of their web browser. By running a series of checks, it reveals which kinds of information such as IP address, browser fingerprint, plugins, WebRTC leaks, and tracking data are being exposed to websites. Key features include:

* A comprehensive dashboard with real-time results.
* Tests for IP address leaks, cookies, plugins, JavaScript, Flash, WebRTC, referrer headers, and more.
* Scoring system to benchmark your browser’s privacy.
* Recommendations to improve browser privacy based on your results.
* No registration or download required; works on any modern browser.

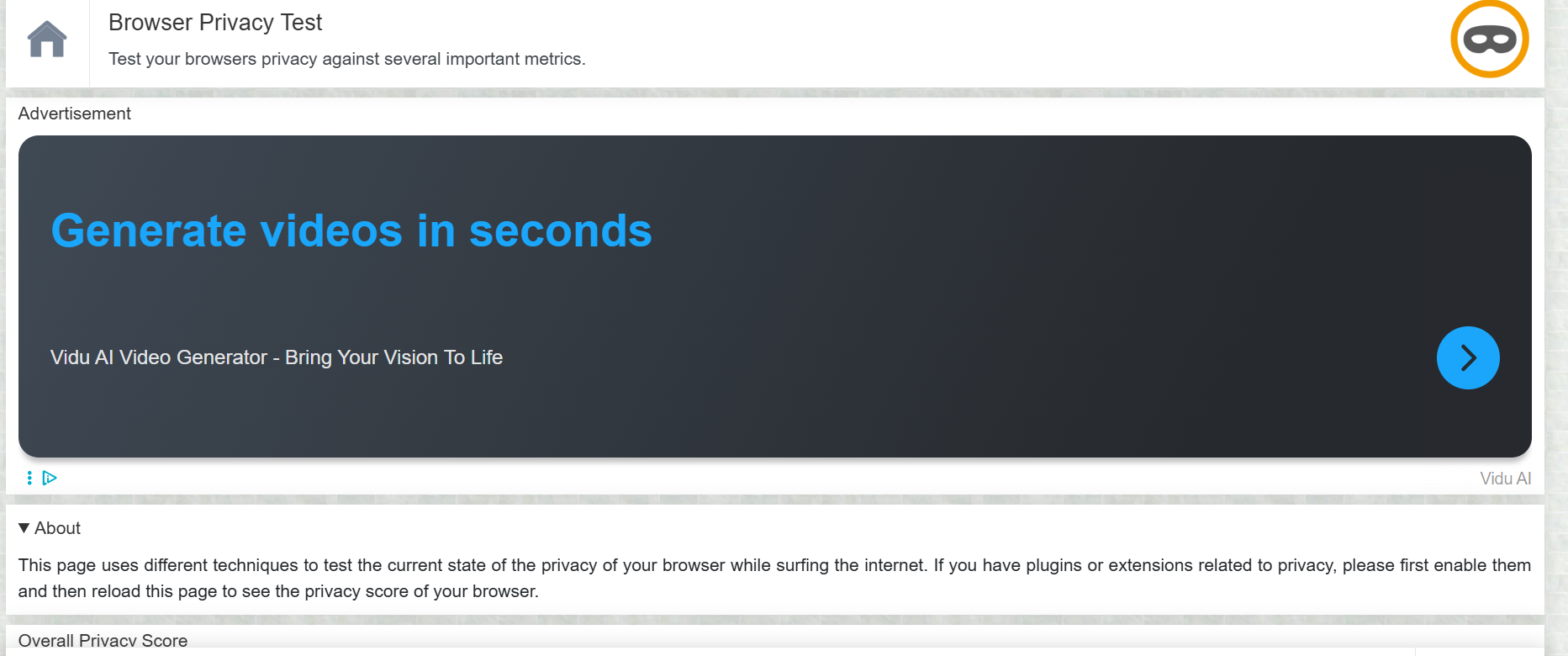
### **Why I Chose It:**

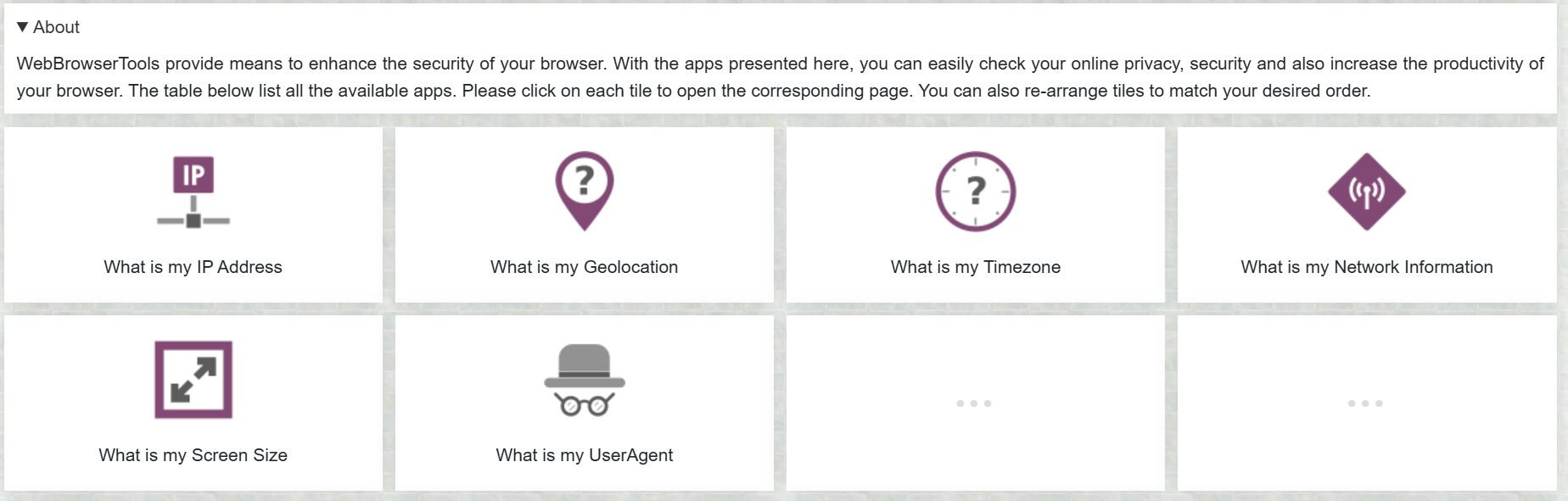
This tool is a classic example of a PET that educates and empowers users. It enables users to see exactly what information their browser leaks and provides actionable advice for improvement. Unlike other PETs that “fix” privacy, this one helps you **understand and manage** your privacy proactively. It’s a great resource for both privacy beginners and advanced users.

## **Task 2: Hands-On/Exploration**

### **How I Set It Up:**

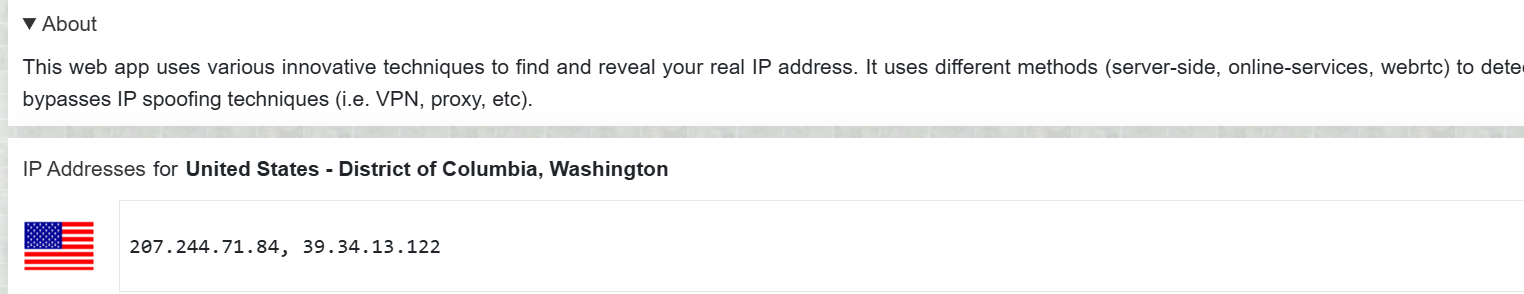
1. Opened <https://webbrowsertools.com/privacy-test/> in Google Chrome.

****

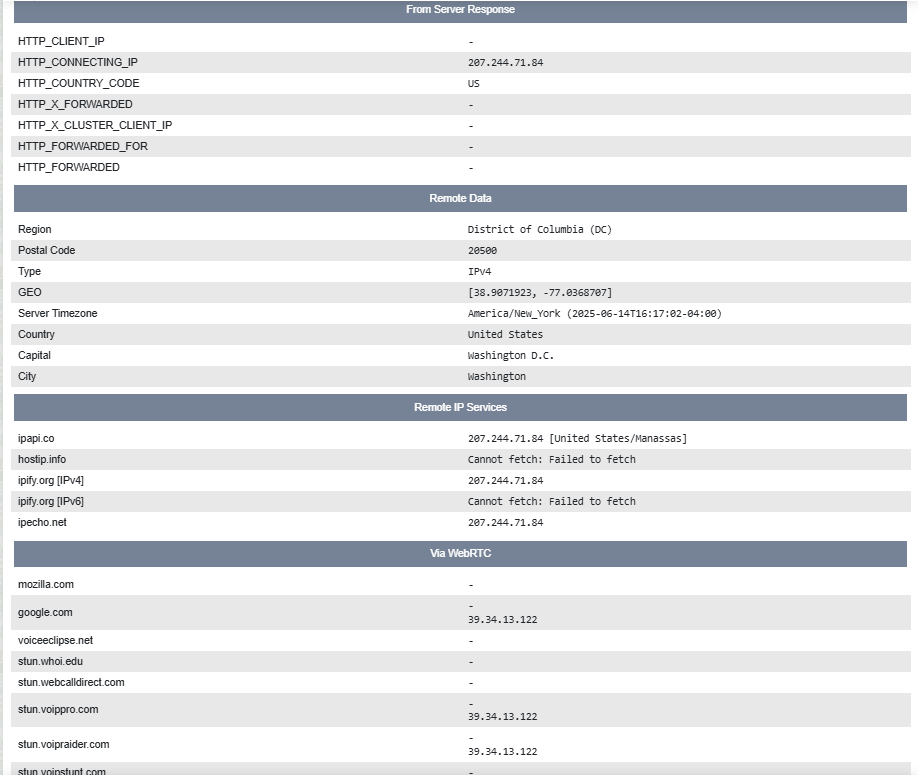
1. Clicked “Start Test” to begin the privacy analysis.  
   ****

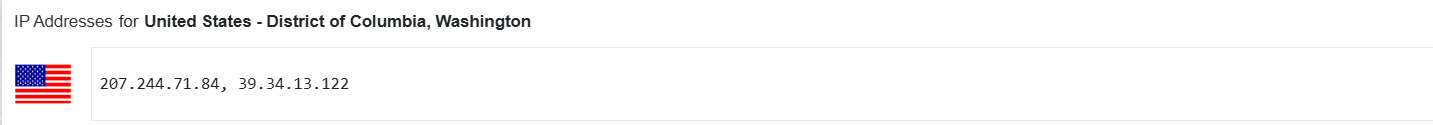
### **What I Did:**

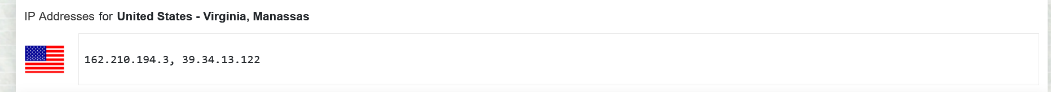
* The test automatically ran a series of privacy and security checks, covering:
  + IP address exposure
  + Browser fingerprinting
  + WebRTC leaks
  + Cookies and local storage
  + Referrer header and JavaScript
  + Plugin and font enumeration



* After a few moments, the results dashboard appeared, showing my privacy score and a summary of findings.



* Scrolled down to see detailed explanations for each test and areas where the browser leaked information.
  + Noticed that my real IP address was exposed via WebRTC, and fingerprinting was possible due to unique plugin and font data.
  + The site also pointed out that “Do Not Track” was not enabled and provided links for further reading.
  + Compared results with the same test in Firefox and Opera (noting that Opera’s built-in VPN helped reduce IP exposure).  
    



### **Observations & Learnings**

* The privacy score provided a helpful “at-a-glance” summary of browser security posture.
* Chrome leaked more information by default compared to Firefox and Opera (especially with VPN enabled in Opera).
* The tool provided clear recommendations for boosting privacy, such as disabling WebRTC, using privacy-focused extensions, and enabling “Do Not Track.”
* The tool is fully free and requires no registration.
* Its simplicity and actionable advice make it an excellent PET for all users.

## **Personal Reflection**

Using the Web Browser Privacy Test was eye-opening, showing how even modern browsers can leak sensitive data by default. It motivated me to review my settings, install privacy extensions, and better understand browser-level risks. This PET is a practical resource for anyone looking to take control of their web privacy, whether at home or work.