# Cookie Monster: Empowering Users to Manage Their Personal Data

Kalyan Karamsetty
kalkaram13@ucla.edu
University of California, Los Angeles
Los Angeles, CA, USA

Beide Liu
beideliu@ucla.edu
University of California, Los Angeles
Los Angeles, CA, USA

Joseph Wong
josephjwong@ucla.edu
University of California, Los Angeles
Los Angeles, CA, USA

## Abstract

In the modern age, many people rely on the Internet to complete everyday tasks. Many sites use cookies to collect data from users for profit through targeted advertising. Many users are unaware of the data being collected from them, despite well-intentioned cookie consent popups due to the European Union's mandated GDPR consumer protection laws. In this paper, we present Cookie Monster: a Chrome extension which provides visualizations of cookies, allows users to manage the cookies on given sites, and provides explanations of the functions of cookies on the site. This extension was developed from the information gathered through the process of user research, which we conducted a survey and follow-up interviews for. We also evaluated our system with several users, where we timed users on specific tasks such as viewing the cookies, blocking undesired cookies, and generating explanations for cookie functions. The extension is built using Svelte with TypeScript and JavaScript for the background service worker. The classification algorithm uses several online databases with known cookie and domain information.

## 1 Introduction

In today's world, the Internet is used for everyday tasks, such as online shopping, banking, booking travel plans, and social media. Every time users visit websites, sites collect cookies from users, which keep track of certain information about the user, allowing sites to sell their data to third parties for advertising. To combat this, the European Union (EU) has privacy laws to protect customers from having their data collected without their consent [3]. As a response to these laws, many sites developed intrusive cookie consent popups, which coerce the user to accept all tracking cookies before allowing them to access the site. Companies which are not bound by these laws continue to collect users' data through tracking cookies without their consent.

Many users, especially those without a technical background, are unaware of the data that sites collect from them. We developed Cookie Monster, a Chrome extension, to help users make informed choices about the data they choose to share with websites. Cookie Monster provides the user with visualizations about the active cookies on a site, as well as the ability to customize their cookie blocking preferences. For the few inclined users, our extension also provides short explanations on the purpose of each cookie identified.

## 2 Problem Statement

Many users are becoming aware of web cookies but lack a clear understanding of their function and implications. According to our user research, about half of internet users recognize the existence of cookies and do not want their personal data being collected. Additionally, many websites query cookie consent through vague and manipulative popups. The users' knowledge of cookies, however, is often superficial, making it difficult for the users manage their cookie preferences.

Users want a convenient and secure browsing experience but are frequently interrupted by cookie consent popups that they do not fully comprehend. Due to their intrusive nature, users often make uninformed choices about the data they choose to share with websites.

## 3 User Research

In order to get an idea of the design space and narrow the scope of our problem, we conducted user research in a two-phase process. First, we sent out a survey to around 25 participants of varying demographics: some users were young, undergraduate students, while others were middle-aged musicians, and others were non-technical parents. After conducting the survey, we decided to conduct several follow-up interviews with users who did not take the survey, now that we had a better idea of user backgrounds and wants.

### 3.1 Survey

The survey had 17 questions, and the questions mostly consisted of general, multiple-choice questions about cookies. The survey started by asking about the users' demographics, including their age and technical background. We asked users to identify whether or not they knew about cookies, and if not, would they like to learn more about cookies. Users were also asked questions about what they would find useful to manage their privacy online, as well as which browsers they frequently use.

The second section of the survey asked users about their experience with cookie consent pop-ups. Users were also asked if cookie consent popups were obnoxious enough to influence them to not use a given site. Finally, users were also asked about their browsing habits: we asked users how often they clear their browsing data, and whether they currently use any extensions or custom browsers to manage their privacy online.

While 79.2% of users wanted more transparency about how cookies are being used on sites (includes users who wanted a general overview or wanted in-depth explanations), only 58.3% of users responded that they wanted to learn more about how cookies work. From our survey results, it appeared to us that there would be significantly more demand for showing users how their cookies are being used rather than educating users about cookies. 95.8% of respondents noted that they found cookie popups to be very annoying, and 70% of users responded 4 or 5 regarding how frequently websites request cookies from them, with 1 being the least frequent and 5 being the most frequent. Around half of the respondents said that they are not likely to avoid a website when they see a cookie popup, while the other half responded that it would influence them to potentially avoid the site.

We found that 83% of users use Chrome, and small percentages (12.5%) used other Chromium-based browsers such as Microsoft Edge and Brave. While a large percentage (62.5%) indicated that they use Safari, given that we only had 25 responses, we suspect that there is a large overlap between the Chrome and Safari users. Given this, we decided that it would be appropriate to create a Chrome extension to address the problems identified from the interview, given that this would also work for the users who are using Chromium-based browsers (though not very necessary for Brave users, as that custom browser has many more privacy features beyond what Cookie Monster provides).

### 3.2 Interviews

We conducted semi-structured follow-up interviews to further scope out our project. We had several base questions that we asked users. These questions mostly included in-depth questions about cookie consent popups, including whether or not users would be more likely click "Accept All" when presented with an intrusive cookie popup. We also provided several ideas to users and asked them whether or not they would find those features useful in a Chrome extension. These interviews also confirmed our hunch from the survey that there are more people who only care about how their data is being used, and not necessarily how their data is being collected from them via cookies.

In the end of the interviews, we found that users would find short and concise visualizations of active cookies on a page to be useful. We also found that users generally wanted a way to customize their cookie preferences without going through the cookie consent popups every single time they visit a site. Users didn't necessarily want a one-size-fits-all extension which blocks all cookies of a certain type; they actually wanted to be able to choose which cookies were enabled on a given page. As a result, we decided that it would be important to also provide users with a short, AI-generated explanation of the purpose of cookies present on a page.

### 3.3 Personas

From our user research, we came up with two personas for our problem.

Our first persona is Jack. He is a typical Internet user who is not technologically well-versed. He uses the Internet for everyday tasks, such as online shopping, news articles, learning new recipes, and social media. While he knows the basics of the Internet, he does not know much about how websites work, and generally will not spend his free time learning about how to better use the technology to meet his needs. He sticks to the same basic tasks on his computer which he is comfortable with. While Jack knows that cookies exist and collect his data, he is unaware of what specific data is being collected from him, and is concerned about the data he shares with companies when clicking "Accept All" on the cookie consent pop-ups.

Our second persona is Alice. She has a bachelor's degree in engineering, and is very familiar with computers and the Internet. She uses the Internet on her phone and laptop extensively through the day for everything from browsing the Internet and online shopping all the way to writing scripts to help her automate mundane tasks. She is aware that cookies collect her data and generally doesn't like this. She would like a quick and easy way to block the cookies she doesn't want tracking her without having to read the details provided in the cookie consent pop-ups.

### 3.4 User Workflow

As in 1, a user will start by visiting a website. On this site, a cookie pop-up appears and asks for the user's consent for cookie usage. This pop-up presents the "Accept All" button very clearly, but other buttons are more difficult to find and understand. In most cases where accept all is clicked, the user either could not find how to exit the cookie pop-up or did not understand the options being presented to them. In both cases, the user made an uninformed choice to accept cookies before being able to continue to the site. Only the users who actually took time to review the options and understood them would go to select their cookie preferences and save them. On some other sites, the cookie consent pop-up is never shown, and users implicitly accept these cookies by using the site.

In all of these cases, users are giving consent for sites to set cookies in their brwoser and collect data through an uninformed decision. Many users do not want to have their data tracked, and Cookie Monster attempts to provide users with the option to make informed decisions about their data.

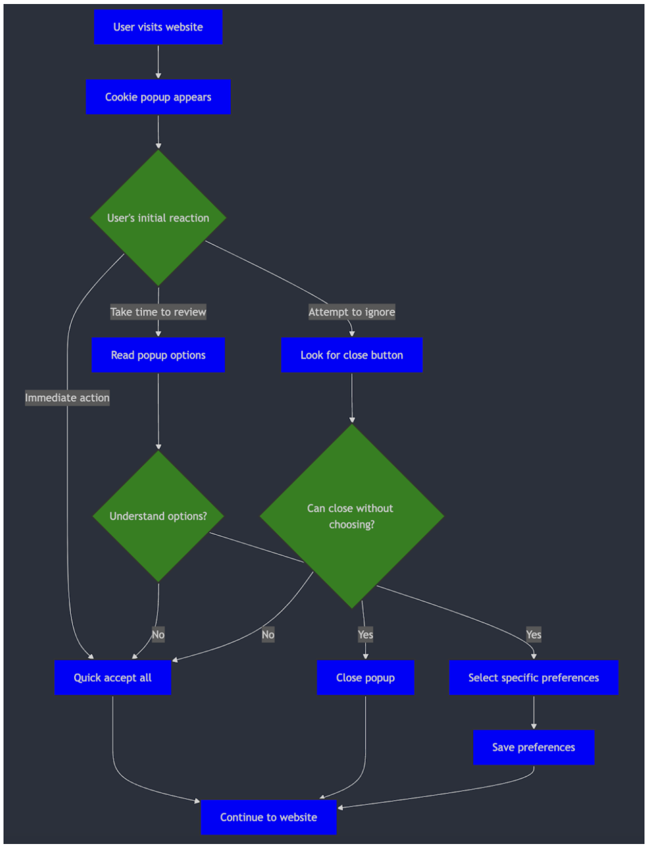


**Figure 1.** User flowchart for the scenario.

# 4 Design Goals

Following the user research we conducted, we came up with the following design goals for our project.

## 4.1 Simple, Concise Visualizations of Cookies

Through giving and receiving feedback with paper prototypes / Figma wireframes as well as interviews, users expressed that they do not want to read a lot of text, and that they will only look at brief snippets in order to manage their cookie preferences. On top of that, we have received from peers that color-coding different cookies might be helpful for the users to recognize different kinds of cookies.

In addition from the feedback from the interviews, we decided to err on the side of brevity for our explanations and interface, opting to provide several groups of cookies, with the option to expand each of these categories and click on individual cookies if a user is truly interested in getting an explanation. To meet this design goal, we also decided to remove technical jargon from all of our explanations, as well as color code cookies and their categories based on their function (with colors like red to indicate harmful cookies, green to indicate necessary cookies, etc.).

We also added a display badge on our extension so that users can see how many cookies are currently active on the site without having to specifically click on the popup.

## 4.2 Customizability of Cookie Preferences

Users should be able to customize the cookies that they want to allow on a site without having to go through the intrusive and manipulative cookie consent popups. Follow-up interviews (and our survey) revealed that users strongly dislike cookie popups, and want to be able to set cookie preferences by default for all sites in one tool. However, users also wanted the ability to customize the cookies they allow on different sites. To achieve this goal, we gave users the ability to manage their cookie block list, which prevents those cookies from appearing on the site again. In the future, we would like to give users the option to block any cookie detected within a category that they do not want to allow.

## 4.3 Simple and Optional Explanations

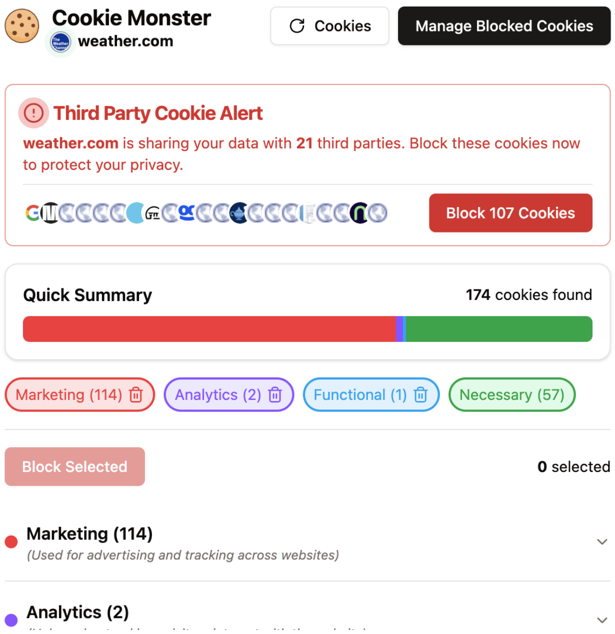
Users should be able to obtain more information about a specific cookie they are managing if they so choose. From the survey feedback, most users expressed that they would like the option to know a little bit more about cookies, but they don't necessarily want to have the explanations to be over the top. Interviews also revealed to us that many users have no desire to learn about the specifics of cookies, but having this option available for users is important in helping them make informed decisions about the cookies they choose to allow or block.

To accomplish this goal, we made each cookie clickable, and used Google's Gemini large language model (LLM) to generate a brief, simple explanation of a specific cookie when prompted to by a user. In the future, we might consider adding a brief description to the manage block list page so that users can easily choose which cookies to unblock on a site.

## 4.4 Easy to Install and Use

Users should be able to easily install and use the system without much disruption to their daily browsing. While there are custom browsers which have similar cookie-blocking features and far more privacy settings than Cookie Monster, making Cookie Monster as a Chrome extension that can be installed in one click would encourage more users to use the extension and be aware of their data. Many users already currently use Chrome, as mentioned from our survey results. Having to migrate to a new browser requires learning how to use the browser from scratch, and importing all previous Chrome settings and passwords into the new browser, a process which can be time-consuming even for those experienced with technology. For a casual Internet browser, this would likely be too much to ask. However, installing an extension in one click would be easy enough that even those who identified as not technologically well versed.

# 5 System Design and Implementation



Cookie Monster
weather.com

Cookies | Manage Blocked Cookies

Third Party Cookie Alert

**weather.com** is sharing your data with **21** third parties. Block these cookies now to protect your privacy.

Block 107 Cookies

Quick Summary — **174** cookies found

Marketing (114) | Analytics (2) | Functional (1) | Necessary (57)

Block Selected — **0** selected

● Marketing (114)
*(Used for advertising and tracking across websites)*

● Analytics (2)

**Figure 2.** The popup which opens when you click on the Cookie Monster extension.

Cookie Monster is implemented as a Chrome extension, and operates in the background with a JavaScript service worker which listens to cookie change events. The extension has a badge which displays the number of cookies active on a site, which refreshes every second. It updates on a set interval to prevent too many Chrome API calls from being made at once when a page attempts to load. These calls are made from the service worker, which checks the number of active cookies every second.

When the pop-up is opened, the extension uses the Chrome API to get all of the cookies active on a site, and displays them in several categories to the user, with a visualization at the top of the active cookies and a blinking red notice when third-party marketing cookies are detected. It does so by first using a script to detect all sites which the current site sent a request to. Then, the extension calls Chrome's cookies API for each of those domains. This is necessary as it is the only way to retrieve *third-party cookies*, which are cookies that are set by third-party sites. [4] These third-party cookies are typically used for companies to collect data and use it for targeted advertising through cross-site tracking. Cross-site tracking is used to collect data about the user's behavior across multiple sites. [5]

## 5.1 Cookie Classification Algorithm

When retrieving the cookies from the Chrome API, the cookies come with only certain metadata, of which the most important is the name of the cookie and the domain of the cookie. In order to determine what category the cookie fits into, we use a weighted scoring system based off of several known clues from the cookie's name and domain.

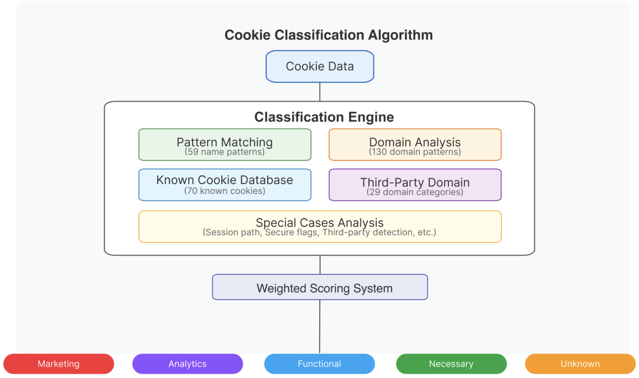


**Figure 3.** Classification Algorithm Diagram.

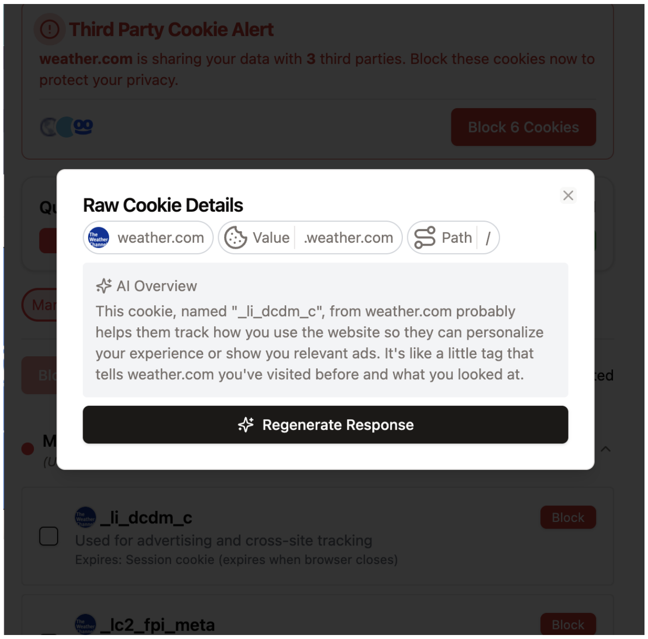
We assign some weight to pattern matching: in other words, if the name of the cookie matches a certain pattern which is typically used in certain categories of cookies. We also use domain analysis (analyzing the domain which the cookie is from) as well as check for whether the domain is third-party. Third-party domains are likely to be marketing cookies due to the possibility of cross-site tracking, as discussed above. There is also a known cookie database which is checked to see if the cookie of interest has been previously identified. Finally, we also weight certain properties about the cookies, such as whether they are secure cookies, session cookies, etc. After taking a weighted sum of the scores, we assign the cookies into one of the four buckets based on which of the four buckets received the highest score, with a fifth bucket for unknown cookies (which is rarely seen).

## 5.2 Cookie Blocking

In order to block the user-selected cookies, a JavaScript service worker runs in the background to intercept the `cookies.onChanged` event. When a site attempts to add a cookie, this event is triggered, and the service worker deletes the cookie immediately. While this is a workaround, this is due to the limitations of Chrome's Manifest version 3. [2] In Manifest v2, we could intercept the headers and prevent the cookie from even being set; [1] however, Google is currently phasing out support for Manifest v2 extensions, so this was not a solution we could pursue. Despite the limitations of Chrome's Manifest v3, this still prevents sites from getting any meaningful data to use for targeted advertising.

## 5.3 Cookie Explanations

In order to generate explanations for users, we use Google's Gemini, a large language model capable of handling these types of questions. We use the following prompt: "In a few



Third Party Cookie Alert

weather.com is sharing your data with 3 third parties. Block these cookies now to protect your privacy.

Raw Cookie Details

AI Overview

This cookie, named "_li_dcdm_c", from weather.com probably helps them track how you use the website so they can personalize your experience or show you relevant ads. It's like a little tag that tells weather.com you've visited before and what you looked at.

_li_dcdm_c

Used for advertising and cross-site tracking

Expires: Session cookie (expires when browser closes)

_lc2_fpi_meta

**Figure 4.** Gemini generated explanation of a specific cookie.

sentences, Explain what this cookie likely does in a short, non-technical user-friendly way. Here are the cookie details." We then provide Gemini with the cookie's name, domain, path, value (up to 100 characters), and the active domain. Since we do not have a secure way of storing our Gemini API key, we currently have a prompt for users to enter their own Gemini key, and provide clear instructions on how to obtain the key. Ideally, if we had a proper secret manager, we would use the secret manager to provide the Gemini key, as this is a hindrance to the user experience.

# 6 Evaluation

We evaluated the system on 10 users by giving them two separate tasks. The first one was to visit weather.com, a site which we discovered to have many tracking cookies. The user was then asked to view the active cookies on a site, generate an explanation for a specific cookie, and delete specific cookies from the site using our extension. Finally, we asked users to navigate to a site of their choice and remove all of the undesired cookies. We timed users on each of these subtasks, in order to get an idea of the proportion of time that was being spent actually blocking cookies vs. viewing the visualizations or learning about the cookies present. We incorporated our instructor's feedback here by considering that measuring time on its own without splitting it up into different subtasks would result in an inaccurate portrayal of evaluation results, as users may spend more time due to getting distracted by reading explanations or viewing other aspects of the interface. We then analyzed the timings we collected from the user by running standard statistics on them: mean, median, standard deviation, as well as quartile information and min/max. Plotting them into histograms helped us see whether there was a large variance due to outlier results or if there was more widespread confusion in using our system. Since we were observing the user while timing them, we also consulted our notes to understand the reason a user was taking a long time on a task.

We also gathered qualitative data by asking the user for feedback about our system: specifically, we asked them to rate our system on usability, meeting the expectations laid out, explanations generated, and the visualization quality. We conducted semi-structured interviews here, where we asked these broad questions and then asked users to explain their ratings. We also followed up on any suggestions the user made in order to see where our system could improve.

Since we conducted evaluations on our own devices to prevent users from having to turn on developer mode and set up a development environment for our extension, we were unable to evaluate the ease of installation component of our design goals, as this would not be an accurate representation of the amount of effort required by a user to use our extension.

# 7 Findings

Overall, we found that our system was very effective in providing users with visualizations of active cookies and allowing users to manage their cookie preferences by blocking undesired cookies.

## 7.1 Quantitative Results

The majority of users were able to view cookies in under 10 seconds; it seems like the large variance and outliers were due the facilitators' different definitions of considering this task being done. Some facilitators considered the task done when the user opened the popup and saw the general summary of the cookies, while others waited until the user clicked into the dropdown menus in order to consider the task done. If we consider only the time it took a user to see the general summary, every user completed this task in under 10 seconds.

There was a large variance in viewing cookie explanations: some users found the explanations in 3 seconds, while other users gave up and never found the explanations without facilitator intervention. One of the takeaways from this result is that we need to add some sort of signifier to show the user that they can interact with the individual cookies. Additionally, there was some variance on the lower end of the spectrum where some users appeared to have accidentally found the "Generate Explanation" panel, so it is not clear whether or not these timings are an under representation of reality.

The median time for deleting cookies was 13.5 seconds, with some variance (up to a max of 32 seconds). The variance was caused by users who used the trash can to delete an entire category of cookies vs. users who deleted cookies one by one. Based on this and user feedback, it seems that it could be more clear that a user can mass delete cookies using the trash can icon in the visualization.

For the task of visiting a website and managing the cookies on the site, the median time was 10.5 seconds. All but one user finished the task in under 30 seconds, with one outlier result of 55 seconds. The majority of the variance in this result is caused by the different preferences of users: some simply deleted all of the cookies they were prompted to by the third-party cookie prompt, while others went one by one to select cookies to block. Very little time was wasted on navigating the interface, and being able to manage the cookies in under 30 seconds for the most part suggests that the interface is straightforward and easy to use.

### 7.2 Qualitative Results

Generally, users found our interface to be very easy to navigate. On a scale of 1 (lowest) - 10 (best), our averages for usability, visualizations, and meeting the expectations laid out were around 9 out of 10. Our average for explanations was lower, at 8 out of 10: some users found that the explanations were too long and not very helpful for them because they would not read such a long blurb of text. They also felt that the short, few word summary in the popup (non-AI generated) was sufficient for them.

In this process, we received a few user suggestions:

- Include cookie function on the block list page so that users can easily see what they are re-enabling.
- Order block list with analytics / functional cookies first.
- Make LLM-generated explanations in more certain terms.

While evaluating our extension, we also noticed a major performance issue on lower end computers. Initially, our cookie extension was retrieving all cookies for the display badge on every `cookie.onChanged` event. However, analyzing the resources retrieved on every cookie change event was far too performance intensive, and we refactored our code to make sure the cookies were only retrieved once a second.

## 8 Discussion and Future Work

Overall, our extension was quite successful in meeting our design objectives: users found our extension to be visually appealing, easy to use, and users felt that the visualizations of the cookies tracking them on a given site helped them make informed decisions about what cookies to allow on the sites they use.

In the process of designing the product, we made several mistakes. One of the first mistakes we made was in the process of our survey: we did not collect the user's email, so reaching out to them for a follow-up interview was not possible. Additionally, our survey was too vague: it provided us some clues as to where to go, but did not really provide us with much of a user scenario. While it provided some insights, our survey could have asked more questions and included a few free-form responses to give us a better idea of what direction to pursue. As a result, we had to conduct follow-up interviews with a new group of respondents. We also went into the user research portion with a problem already in mind, so our scope was narrower than it could have been, and perhaps we could have addressed more problems.

Due to time limitations, we were not really able to parallel prototype as we would have liked - as a result, our product went in one direction. We focused on the visualizations and display badge in our extension, and failed to address one of the major annoyances from users: the cookie consent popups. Being able to parallel prototype and gather more users to test the prototypes would have given us more insights into what worked and what didn't; incorporating this feedback would have (hopefully) resulted in fewer suggestions from users during the pilots and evaluations.

There are still several improvements we would like to make to the extension, and here are some of them:

- Include a preferences page, so the user can choose to block all cookies in a certain category by default without having to manually manage the cookies on each site they visit.
- In user research, many users stated that cookie consent popups were extremely annoying. We would like to inject some content script to automatically block those pop-ups and allow users to manage their cookies through our extension.
- Include cookie function on the block list page so that users can easily see what they are re-enabling.
- Categorize blocked cookies into groups on the block list page. This is essential for making users have an easier time to re-enable certain cookies and find the cookies they want to re-enable.
- Incorporate a secure way of storing one common Gemini API key, so that users don't have to create their own key to use the extension for explanations. While this is not the biggest inconvenience, it could be a hassle for someone who isn't too familiar with technology to do this.
- Include a signifier to indicate to the user that they can click on the individual cookies to generate explanations. Some ideas would include making the cookie entry change color (to blue, for example) and changing the cursor to a pointer when hovering over the item.

## References

[1] Chrome Developers. 2025. *webRequest API.* https://developer.chrome.com/docs/extensions/reference/api/webRequest Accessed: 2025-03-18.

[2] Chrome Developers. 2025. *What Is Manifest V3?* https://developer.chrome.com/docs/extensions/develop/migrate/what-is-mv3 Accessed: 2025-03-18.

[3] GDPR.eu. 2025. *What Is GDPR?* https://gdpr.eu/what-is-gdpr/ Accessed: 2025-03-18.

[4] Mozilla Developer Network. 2025. *Third-Party Cookies*. https://developer.mozilla.org/en-US/docs/Web/Privacy/Guides/Third-party_cookies Accessed: 2025-03-18.

[5] NordVPN. 2025. *What Is Cross-Site Tracking?* https://nordvpn.com/blog/cross-site-tracking/ Accessed: 2025-03-18.