HERIOT WATT UNIVERSITY

Taming the Cookie Monster – An Analysis of Automated Cookie Management

Callum Duncan Forsyth

BSc (Hons) Computer Science

Final Year Dissertation

Supervised by Prof. Manuel Maarek

April 2022

Declaration

I, Callum Duncan Forsyth confirm that this work submitted for assessment is my own and is expressed in my own words. Any uses made within it of the works of other authors in any from (e.g., ideas, equations, figures, text, tables, programs) are properly acknowledged at any point of their use. A list of the references employed is included.

Signed: Callum Duncan Forsyth

Date: 21/04/22

Acknowledgements

Abstract

Cookies are currently one of the most invasive and convenient ways of tracking a user's browser interaction. Despite new General Data Protection Regulations (GDPR) cookie tracking continues to evolve and bring new security and privacy concerns. This concern establishes a need for new user friendly, privacy friendly useable security.

This project aims to provide a user and privacy friendly automatic cookie manager that helps users manage their interactions with websites. The tool follows the users' selection establishing preferred behaviour and providing them with a more straightforward way to interact with cookie banners. The final result is a Google Chrome browser extension that will be available for download on the Chrome Web Store pending approval.

Table of Contents

Table of Figures

Table of Tables

Chapter 1 Introduction

The use of computers has continued to grow with each generation of the population, no longer are computers cumbersome technical machines that require prior knowledge to operate. In today's age computing devices are extremely user friendly and have now become a part of everyday life. Web browsing is used in every aspect of our lives, from personal knowledge to education and work, we are increasing sharing more information than ever before. User data has become a currency of sorts with companies continually inventing new ways to build user profiles and collect sensitive information. There is an increasing number of predatory webpages seeking to exact a user's personal information with no real boundaries on what they can and can't do with it.

Despite the introduction of GDPR webpages still continued to collect user data simply by making it quicker and more convenient to give full consent rather than informing their customers of the consequences that continually accepting all cookies has. This begs the question; just how much data is willingly handed over to advertisers and corporations without our knowledge and understanding.

1.1 Motivation

"Since the adoption of the General Data Protection Regulation (GDPR) in 2018 more than 60% of popular websites in Europe display cookie consent notices" [5] often in the form of a cookie banner, these consent notices have plagued users' screens and continued to build a fatigue of privacy acceptance. Users are tired of constant bombardment to adjust their cookie preferences and often accept the quickest option, full consent. This frustration demands a solution that allows users to set their consent once and continue browsing the web freely without constant interruption. A successful solution must provide users with a tool that does not compromise useability over privacy, and rather allows the user to make informed decisions through education, as well as being useable as to not frustrate the user back into unnecessarily giving away their data out of convenience.

1.2 Aims

The aim of this project is to develop a user and privacy friendly tool that automatically deals with a user's cookie interactions while web browsing. Along with automatically sorting cookies the tool will allow the user to set predefined settings and choose browsing modes. In order to educate the user regarding the amount of data currently being tracked the tool will provide information on different types of cookies and their purpose. This provides a unique opportunity that allows the user to specify the level and type of cookie tracking they are in favour of. This benefits users that value their privacy above all and choose to reject cookies as well as users that enjoy more convenience and personalised advertising.

1.3 Objectives

The projects main objectives are summarised by category as follows.

1. **Align the tool with current GDPR policy. (Policy Alignment)**

   The tool being developed must follow current GDPR policy and not add to the problem of taking more user data than necessary.

2. **Allow users to make informed decisions regarding the level of cookie tracking. (Informed Decisions)**

   The tool must provide some form of education to ensure the users have the tools necessary to make informed decisions when browsing the web.

3. **Educate the users based on their chosen settings. (Education)**
   The tool must also provide the user with information regarding the consequences of their chosen selection.

4. **Allow users to automatically sort cookies based on their preferences. (Development)**
   The tool must follow the user's selection and allow them to set their preferences once and browse the web freely without continued interferences.

5. **Ensure the tool is accessible and useable. (Useability)**

The tool must be useable enough such that it does not cause the user to revert back to manually interacting with cookie banners out of frustration with the tool's useability.

Chapter 2 Background

This section will present and discuss the current research in relation to this topic. This projects aim is to create a user and privacy friendly tool to automatically deal with cookie requests. The research areas surrounding this topic include a review of cookies (see Section 2.1) and General Data Protection Regulations (see Section 2.2). The effects GDPR has had on cookie tracking will also be discussed (see Section 2.2) as well as a review of other methods of useable security (see Section 2.3).

2.1 Cookies

In today's age of modern computing cookies are one of the most useful ways a website can learn information about a user. A cookie is a small text file that gets saved on a user's computer, specifically their hard drive. The cookie is saved by a web server to the user's device when they access the webpage. Although cookies have many different functions their main task is to store information on their users, this can be anything from their page preferences to coupon codes and login details, this information is then stored in name-value pairs (see Figure 1).

	Domain	Flag	Path	Cookie_Name	Cookie_Value	Secure	Date
Cookie 1	acme.com	True	/	Name_Cookie	Alice	False	12/31/2000
⋮		⋮			⋮		
Cookie n	acme.com	True	/	Role_Cookie	Manager	False	12/31/2000

Figure 1 - An example of cookies [20]

Cookies have come a long way from their initial development in 1994, they were first intended to help users while online shopping by storing recently viewed items. Lou Montulli, the creator of cookies defined them as a "piece of data that is stored, then given by the server to the client, stored by the client, and returned to the server each time the client returns" [1]. Cookies were originally used as what most would call a 'basket' today, this is still one of their purposes however as with all technology they have evolved, becoming something much more sinister.

13

Cookies have now moved beyond basic user customizations and are beginning to store more and more intrusive information, often without the users consent or knowledge. This information can be used by advertisers to display personalised and targeted marketing material to unsuspecting users. Although cookies do serve a useful purpose, most websites would not run correctly without the use of at least some cookies, however due to the introduction of mass targeted marketing, cookies have become a double-edged sword.

If you visit a music website to listen to a new song, the website will store information on you in order to recommend other music and artists that you may like, this on the surface seems like a great idea, the user gets songs that they a more likely to enjoy and the website gets increased traffic in the form of customers returning to use their site, however, that same information stored on the users music taste can now be sold to third party advertisers that will bombard the user with all kinds of marketing material, from band merchandise to instruments and even tour dates in their local areas; based off of the users IP address. Some people like the thought of being automatically shown their favourite bands new t-shirts and also being the first to be told about an upcoming tour, however, this was all being done without both the user's knowledge or consent, until the introduction of the General Data Protection Regulations.

2.2 Effects of GDPR

Increased internet traffic has left companies with the complex task of evaluating whether their methods of data collection are legally compliant. Over the past decade online activity has greatly increased and data has become a valuable asset, even being called the currency of the future [2]. In order to protect users and increase privacy, the European Union (EU) introduced the General Data Protection Regulation (GDPR) on the 25th of May 2018.

The new regulations are not limited to companies that operate within the EU; in fact, the regulations cover a wide scope reaching as far as to include websites that can be visited by EU members regardless of the company's physical location. Although GDPR has a large scope and includes regulations for data stored both offline and online, data obtained through the use of cookies is focused on two main issues, the conditions for consent [3] and the principles relating to the processing of personal data [4].

GDPR has had a considerable effect on the use of cookies for EU users, not only has it effected the way cookies are stored and processed, but more importantly it has given the user more control over their personal data.

In general website cookie notices fall into four categories, the first is when a website gives a user the option to change their cookie settings, this can include accepting all cookies, rejecting all cookies, or adjusting their preferences to suit. The next category is websites that alert the user to the use of cookies but do not allow them to adjust their settings, this means the user either chooses to use the website with the cookies stated or not at all. Next are websites that do not allow EU visitors at all, often this is to avoid having to deal with EU and non-EU visitors separately, the most popular example of this is American news site Los Angeles Times (see Figure 2). Finally, there are websites that do not display any kind of cookie notices to their visitors.
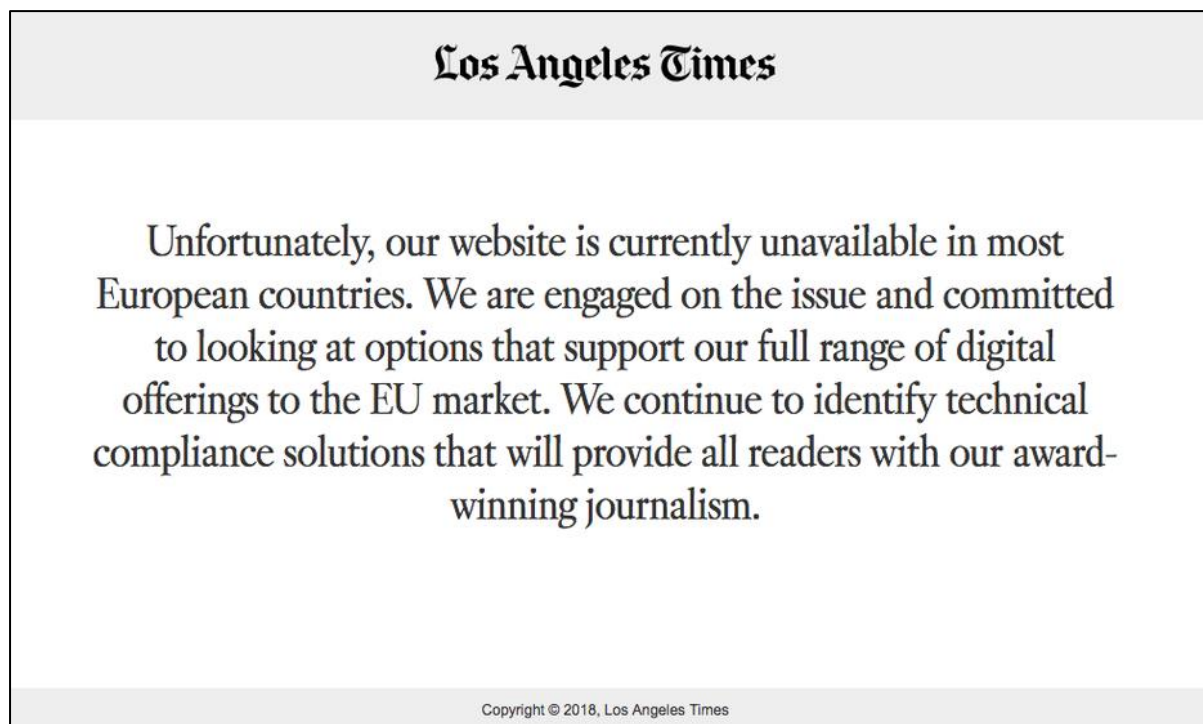

Figure 2 - LA Times rejects EU visitors [22]

Most research is centred around the Alexa.com list of top websites with studies showing that around 80% of websites in the UK showed some form of cookie noticed after GDPR came into effect, with only 22% of websites choosing not to show a cookie notice at all [24]. Although this data shows a clear improvement for users it does not show if the number or types of cookies has changed since GDPR's introduction. In 2018 research was conducted using the Alexa top 1000 world websites, this study showed that 49.3% of cookie-using websites choose not to set cookies without the users consent when the visitors were from the EU, this however was not the case with visitors from outside of the EU [6].

Despite GDPR being an EU regulation and primarily having an impact on visitors from the EU there has also been some positive changes for non-EU visitors. This is largely in part due to websites avoiding the added work of dealing with the two parties separately, rather than displaying cookie notices and only using certain cookies with part of their visitors, some websites have chosen to brand all visitors under the same rules regardless of where they are from. When comparing data from 2016 to 2018 research shows that cookie load was reduced by up to almost 47% for US customers [6].

GDPR has also affected the number of websites globally that display cookie banners, data shows that the number of websites displaying cookie settings options are very similar between the EU and the US, with a cookie notices appearing in 32% of US-based websites despite there being no legal requirement to display them [7]. Interestingly when users take advantage of third-party services such as *networkadvertising* [8] or *TRUSTe* (see Figure 3) [9]; sites that allows users to opt-out of multiple tracking companies at the same time and focus on compliance with GDPR, they are tracked less when browsing 41% of Chinese websites, again despite China have very little cookie control [7].

Figure 3 - TRUSTe framework [9]

2.3 Useable Security

The research is clear that GDPR has increased the number of cookie notices for users on the web, however, an increase in cookie banners has also brought the opportunity for websites to make use of "dark patterns", these are "tricks used in websites and apps that make you buy or sign up for things that you didn't mean to" [10]. In terms of cookie notices there are many ways websites employ dark patterns, this can be a large "Accept All" button in comparison to a very small "Reject All" or the use of contrasting colours to focus the user's eye on an acceptance button. One website that was tested made users click through seven different cookie notices in order to reject cookies successfully, in contrast
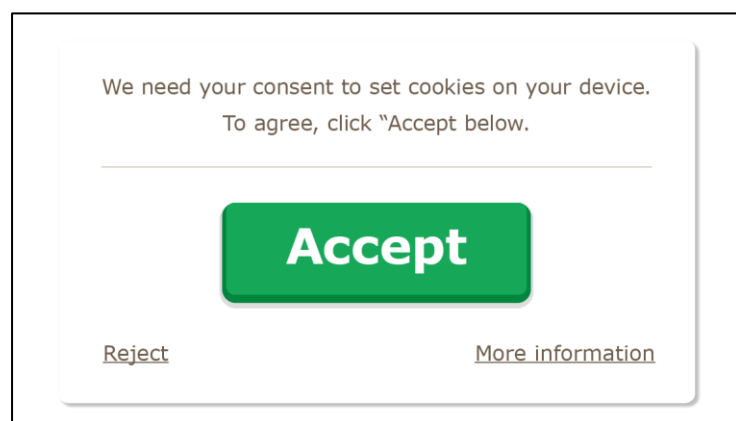
Figure 4 - Cookie banner using dark pattern [21]

the user was able to click the accept button once and was directed straight to the site. There are many examples of websites tricking users into consent or simply confusing them so much it's easier to accept

17

all cookies than select their preferences, one popular news site forced users through 25 pages of content before they were able to opt out of cookie tracking [7].

Websites have demonstrated it is advantageous to have their users accepting all cookies and research shows there are many different tactics to increase the chances a user gives full consent, not only do websites make it confusing for users to opt out, there is also very little information available for users to educate themselves on what certain types of cookies actually do. A recent collection of studies asked 94 participants the question "What do you think happens when you click decline?", the most prominent expectation was that rejecting cookies would stop users from being able to access the website, with the second most common answer being participants expected parts of the website not to work [5].

An increase in cookie notices as well as an increase in dark patterns has led to a need for privacy friendly useable security, currently there are options available that allow users to automatically deal with cookie requests, however, the most popular tools only allow users to either accept all (see Figure 5), reject all or simply hide the cookie banner and don't actually change any settings [11].
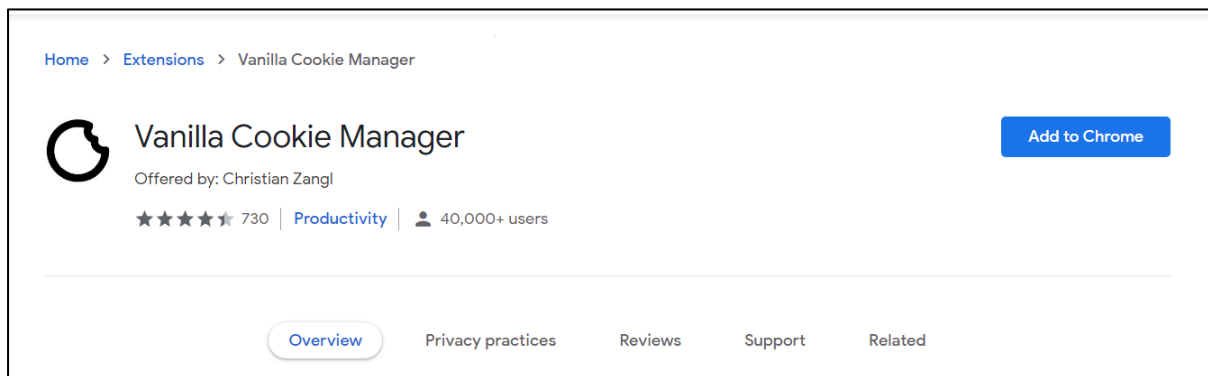
Figure 5 - Most popular Chrome Store cookie manager [11]

There is continued debate on what makes a new design better in terms of useable security, Kai-Ping Yee's work is among the most cited [12] and focuses on addressing "valid and nontrivial concerns specific to useable security design" [13]. Yee's principles can be summarised into ten main points [14], this project will focus on two of them.

Active authorization - "Grant authority to others in accordance with user actions indicating consent"

[13]

Foresight - "Indicate clearly the consequences of decisions that the user is expected to make." [13]

It is important to provide users with the ability to complete tasks using the least path of resistance, this can include giving users all of the information they need presented in a clear and understandable format. An example of good design is the Salmon File permission interface [13], this was developed to replace the standard Windows XP file permissions interface and followed all ten of Yee's useable security principles, research showed a 94% reduction in errors when using the new interface [13].
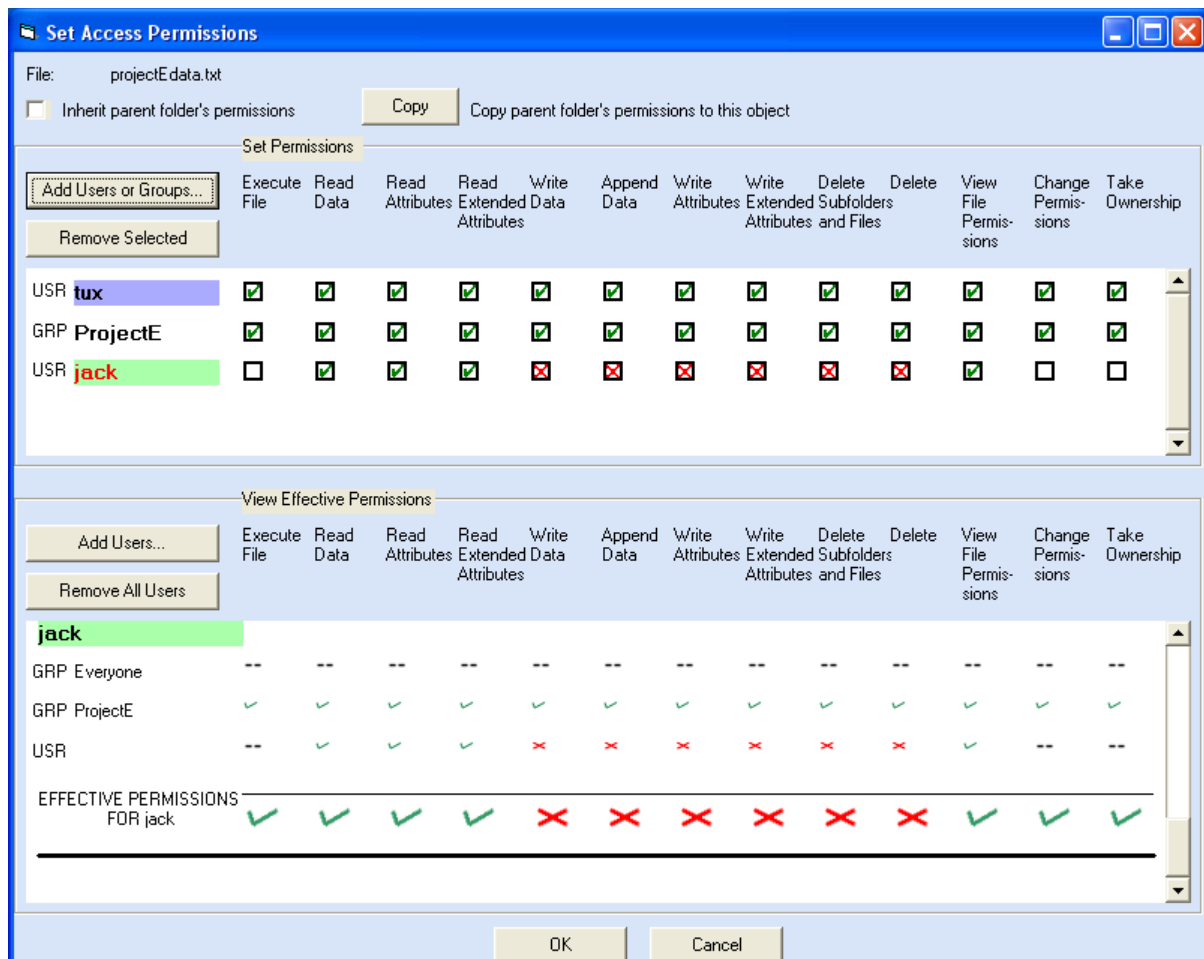
Figure 6 - Salmon File permission interface [13]

2.4 Conclusion

GDPR was set out by the EU to help regain the public's trust and show that they are treating personal data responsibly, with marketing companies bidding for customer data and personal information now more valuable than ever the new regulations have changed the landscape of cookie tracking and online consent forever. With an increase in GDPR consent notices comes a need for more useable security, it is important to provide users with simple, useable tools that educate them on what data they're allowing websites to access.

Chapter 3 Requirement Analysis

This chapter covers the requirement analysis of the tool, both functional and non-functional are discussed. All requirements contain an identifier, a priority (see Section 3.1) and a description.

3.1 Priority Scheme

Must Have: Requirements that must be implemented to provide core functionality in the final system. These requirements are high priority and will be developed first.

Should Have: Requirements that should be implemented and functional in the final system. These will be developed after all 'Must Have' requirements are implemented.

Could Have: Requirements that could be implemented in the final system to add functionality. These are the lowest priority and will be developed after all other requirements have been implemented.

Won't Have: Requirements that will not be included in the final system.

3.2 Functional Requirements

This section covers the functional requirements of the tool. Each requirement (shown in Table 1) includes a functional requirement identifier (FR – ID), a summary and priority.

Section 5.7 displays a requirements summary table detailing each requirements implementation, evaluation, and their **completion status.**

ID	Requirement	Priority
FR1	Tool must allow user to select level of cookie protection.	Must Have
FR2	Tool must automatically reject/accept cookies based on user selection.	Must Have
FR3	Tool could allow users to blacklist certain URLs.	Could Have
FR4	Tool could allow users to whitelist certain URLs.	Could Have
FR5	Tool could allow users to delete blacklist/whitelist URLs.	Could Have
FR6	Tool should allow users to select between a light or dark theme.	Should Have

FR7	Tool could display the number of cookies rejected.	Could Have
FR8	Tool must be able to be disabled by the user.	Must Have
FR9	Tool could show the type of cookies that are being blocked	Could Have
FR10	Tool could allow users to select a certain browsing mode.	Could Have
FR11	Tool could allow users to clear cookies at the end of their browser session.	Could Have
FR12	Tool could allow users to download their whitelist/blacklist URLs.	Could Have

Table 1 - Functional Requirements

3.3 Non-functional Requirements

This section covers the non-functional requirements of the tool. Each requirement (shown in Table 2) includes a non-functional requirement identifier (NFR – ID), a summary and priority.

ID	Requirement	Priority
NFR1	Tool must be compatible with Google Chrome browser.	Must Have
NFR2	Tool should be simple to navigate.	Should Have
NFR3	Tool could give user educational prompts when choosing settings.	Could Have
NFR4	Tool should not greatly increase browser loading times.	Should Have
NFR5	Tool must be GDPR compliant.	Must Have

Table 2 - Non-functional Requirements

3.4 Requirements and Objectives

This section covers the relationship between the requirements and the objectives set out in the introduction (Section 1.3)

	Objective type				
Requirement	Policy Alignment	Informed Decision	Education	Useability	Development
FR1					X
FR2		X			X

FR3					X
FR4					X
FR5					X
FR6				X	
FR7			X		
FR8					X
FR9			X		
FR10		X			
FR11					X
FR12					X
NFR1					X
NFR2				X	
NFR3		X			
NFR4					X
NFR5	X				

Table 3 - Requirements and objectives relationship

Chapter 4 Implementation

4.1 Overview

This chapter covers the implementation of the tool – the languages and libraries used, the reasoning for choosing them and the process of developing the tool.

4.2 Architecture

There are multiple different segments to the project, to simplify, the main implementation is divided into two sections: the tools interface and the background scripts.

For both sections compatible languages have been used, the background scripts are primarily written in JavaScript [15] due to its large number of libraries, interactive behaviour and extensive documentation online.

The interface is written with HTML5 [16] and CSS [17] without any additional frameworks, this was done to avoid any potential compatibility issues and prevent unnecessary responsive scaling.

Below shows the tools architecture describing the interaction between different components. The tools interface contains three pages, Popup, Settings, and Info. All background scripting done using two scripts, a content script used for injection and a main script housing the tools functionality. The users' selections on the interface are recorded using Local Storage Flags and conditional statements.
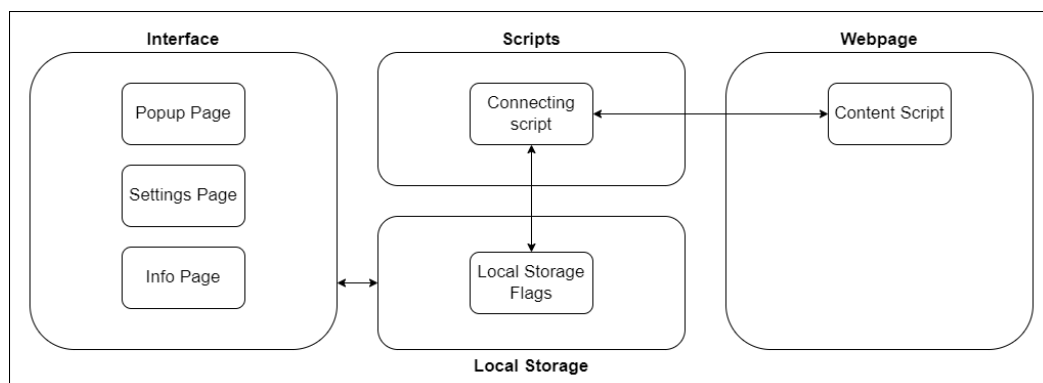

Figure 7 - System Architecture

4.3 Development Environment

As the languages chosen do not require a specific operating system to run, the development environment was split over two different systems, the Heriot Watt Linux OS and Windows 11. The majority of the code base was written using Visual Studio Code [18] as it is optimized for building and debugging modern web applications.

Chrome DevTools [19] was also used throughout the development to inspect and debug various functionalities. Chrome DevTools is an array of web developer tools that are built directly into the Google Chrome Browser, the tools are particularly important when searching for the ID's and classes of various input types (see section 4.5.2).
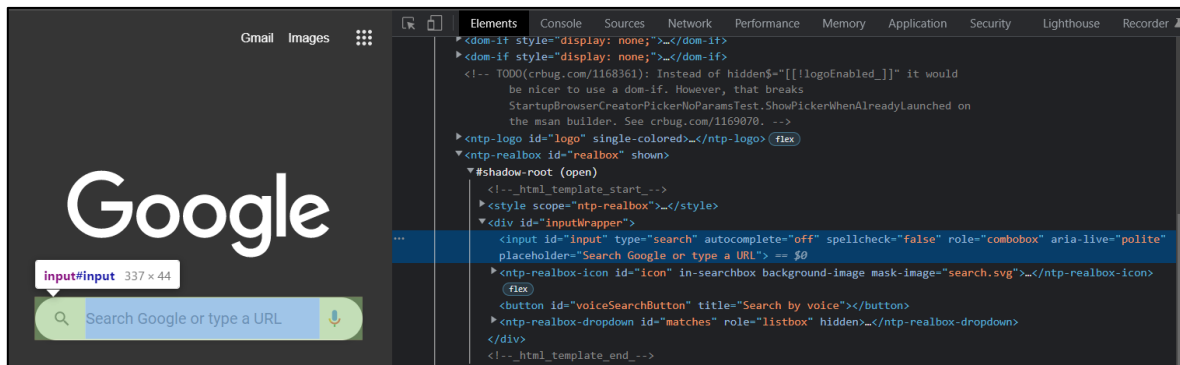

Figure 8 - Chrome DevTools ID/Class search

DevTools application section allows for an in-depth analysis of cookies currently used by the browser, these can be sorted by various metrics and were used to ensure the extension was achieving the previously set objectives (see Section 1.3).

Figure 9 - Chrome DevTools Application Cookie Filtering

4.4 Chrome Extension

4.4.1 Google Chrome Browser

The tool was developed to be compatible with Google Chrome Browser as stated in NFR1. Google Chrome was chosen as it has the largest market share at 59.7% compared to other mainstream browser such as Firefox, Microsoft Edge, and Safari [25]. Chrome browser encourages developers to use their extensive Chrome DevGuide as well as their Chrome DevTools functionality, allowing developers to build a range of different extensions using relatively simple technologies as mentioned in section 4.2.

4.4.2 Content Scripts

Content scripts are JavaScript files that execute in the context of a web page. The scripts use the Document Object Model to read the details of a web page, make changes to the page and pass information from that page to a browser extension. A content script differs from regular JavaScript files as they are executed in an isolated container, this allows them to make changes to its environment without any conflicts from the page itself. The isolated container is a private execution environment that is not accessible by the page or another extension, this means variables in an extensions content scripts are not visible to the host page.

4.4.3 Script Injection

Script injection allows an extension to make changes to another page's CSS and HTML elements. It is used in this context to select checkboxes and click buttons automatically (see Section 4.5.2). Statically declared scripts are registered in the manifest file under the "content_scripts" field (see Figure 10), when declared statically the content script is set to auto run and thus must also contain a matching statement specifying the URL the content script will be injected into. All Chrome extensions contain a JSON-formatted manifest file. The manifest.json is a mandatory file that defines the extension, it contains identity information such as the name, description and version number, it also defines the extensions permission and the actions for its content scripts.

```
     You, 1 hour ago | 2 authors (Callum Forsyth and others)
 1   {
 2       "name": "Cookie Manager",
 3       "description": "Automated cookie manager",
 4       "version": "1.0",
 5       "manifest_version": 3,
 6       "content_scripts": [
 7           {
 8               "js": [
 9                   "content_script.js"
10               ],
11               "matches": [
12                   "https://wordpress.com/"
13               ]
14           }
15       ],
16       "web_accessible_resources": [
17           {
18               "resources": [
19                   "script.js"
20               ],
21               "matches": [
22                   "https://wordpress.com/*"
23               ]
24           }
25       ],
```

Figure 10 - JSON Manifest File

4.5 Core Functionality (Scripts)

The tool was implemented using HTML5, CSS and JavaScript. The content and design were created using HTML and CSS where JavaScript provided the functionality of the tool. JavaScript background scripts are used to automatically select and click elements of a webpage based on the user selection from the tools interface. Scripts are split into two main elements, the content script (section 4.5.1) that injects another script into the webpage, and the connecting script (section 4.5.3) takes the users selection and selects elements of the chosen webpage.

4.5.1 Content Script - content_script.js

This content script directly interacts with the webpage that the user is currently on, it injects itself if the pages URL matches the URL specified in the 'matches' field of the manifest file. It is possible to change single elements by injecting CSS that replaces or modifies current elements on the webpage.

```
{ // Block used to avoid setting global variables
  const img = document.createElement('img');
  img.src = chrome.runtime.getURL('logo.png');
  document.body.append(img);
}
```

Figure 11 - Inserting an image into a webpage

To access and modify multiple elements at once, as well as modify them in a particular sequence it is necessary to inject a whole other JavaScript file rather than just a singular element. This is done using the chrome.runtime API, which allows for a script to be injected when the webpage is loaded,

```
1   var s = document.createElement('script');
2   s.src = chrome.runtime.getURL('script.js');
3   s.onload = function() {
4       this.remove();
5   };
6   (document.head || document.documentElement).appendChild(s);
7
```

Figure 12 - content_script.js'

4.5.2 Accessing Elements

The tool must automatically click the elements of a cookie banner based on the selection the user has made from the interface. Accessing the elements of a webpage is done with the use of query selectors to run the injected code from the background script. Chrome DevTools was used to first identify the class of each element on the banner. This process is done manually by searching the webpage using DevTools inspect functionality to find the correct class name for a given element.
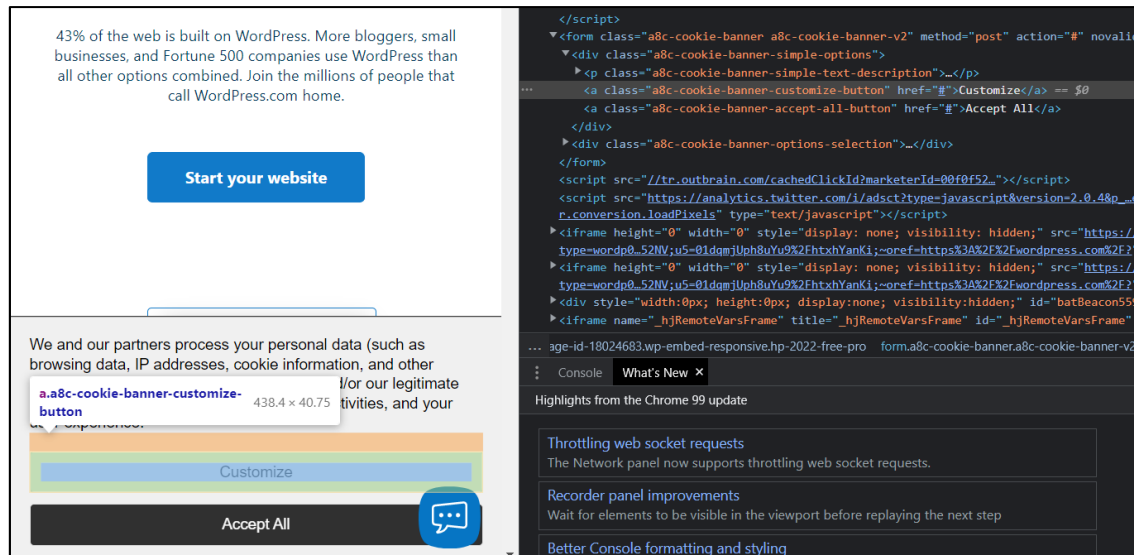
28

Figure 13 - Identifying the class name of the customize button

Once the class is known the button can be clicked by using the Document Query Selector method to references the correct element and HTML click event to simulate a mouse click on the button.

```
document.querySelector("#wpcom-home > form > div.a8c-cookie-banner-simple-options > a.a8c-cookie-banner-customize-button").click();
```

Figure 14 - Clicking button using document query selector

4.5.3 Connecting Script – script.js

The main functionality of the tool comes from the connecting script. 'script.js' is used to connect the tools user interface to the background functionality, incorporating all the previous functionality mentioned in section 4.5.2. There are three main operations happening in the background script, firstly listening for the user's selection, changing the user interface to reflect their selection, and finally managing the user's cookies based on their selection.

Event handlers are used by implementing the '.addEventListener()' method of the web API [26] in order to listener for the user's selection on the interface. The event listeners are activated when the user clicks on the tool's icon in their web browser, depending on the exact element the event listener waits for a button click or a variable change.

```
// ACTIVATE COOKIE MANAGER BUTTON
   document.addEventListener('DOMContentLoaded', function() {
     var checkButton = document.getElementById('activateCookieManager');
     checkButton.addEventListener('change', function() {
```

Figure 15 - Event Handler for User Selection

Once the user has made their cookie selection it is important to update the interface to reflect this change. This is done using the Document Object Model Web API by implementing various methods depending on the element the user has selected. To change the interfaces button selection shown in Section 4.6.1, the '.getElementById()' method is used to select the button, an event listener is then created to listen for any changes as described above and then a conditional statement is used to either check and or disable the button based on the user's selection.

```
// EVENT HANDLER FOR ESSENTIAL ONLY COOKIES BUTTON
document.addEventListener('DOMContentLoaded', function() {
  var checkButton = document.getElementById('essentialOnlyCookies');
  checkButton.addEventListener('change', function() {
    if (checkButton.checked){
      let essentialCheck = true;
      console.log("Essential Only  button = " + essentialCheck);
      document.getElementById("allowAdvertisingCookies").disabled = true;
      document.getElementById("allowAnalyticCookies").disabled = true;
      document.getElementById("allowAdvertisingCookies").checked = false;
      document.getElementById("allowAnalyticCookies").checked = false;
    }
    else{
      document.getElementById("allowAdvertisingCookies").disabled = false;
      document.getElementById("allowAnalyticCookies").disabled = false;
    }
  }, false);
}, false);
```

Figure 16 - Changing the Interface after User Selection

Finally, the most important aspect of the connecting script is to change the web pages cookies based on the user's selection, this incorporates all of the above-mentioned functionality. To keep track of the current selection on the interface, local storage flags are used. When the user selects a certain type of cookies or browsing mode that corresponding flag is set to either true or false. Conditional statements and query selectors are used in conjunction to select elements on the cookie banner in a particular

sequence based on the user selection. An example sequence is shown below based on the test environment TE2 described in Section 5.3.

The actions in **red** show the sequence that takes place on the webpage's cookie banner using the background script, whereas the actions in **blue** show the sequence that take place on the user interface.
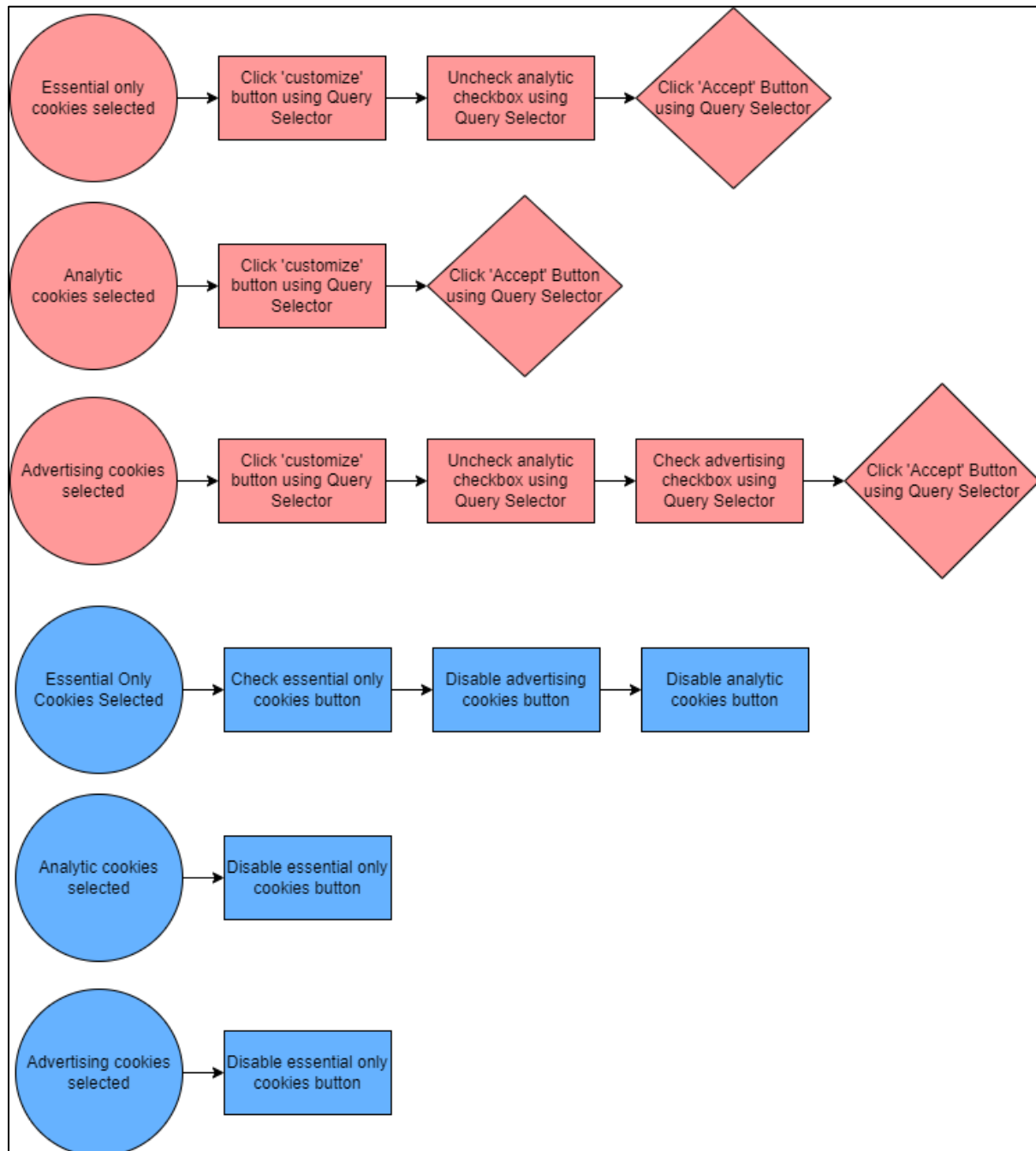

Figure 17 - Script & Interface Sequence

4.6 Interface Functionality

The interface is the connection point between the user's selection and the background scripting functionality, it allows the user to personalise their cookie preferences within set boundaries. The tool can be run in a certain browsing mode (see Section 4.6.1), or the user can individually select the types of cookies they allow. This section details the interface functionality and describes how the tool meets the following requirements: FR1, FR3, FR4, FR5, FR6, FR8, FR10, FR12.

4.6.1 Popup Interface

The popup was designed to give a quick view of the current settings the user has selected and easy access to the change their current browsing mode or cookie selection, satisfying requirements FR1 and F10. The popup page also allows the users to enable and disable the tool efficiently with the click of one button, satisfying requirement FR8.
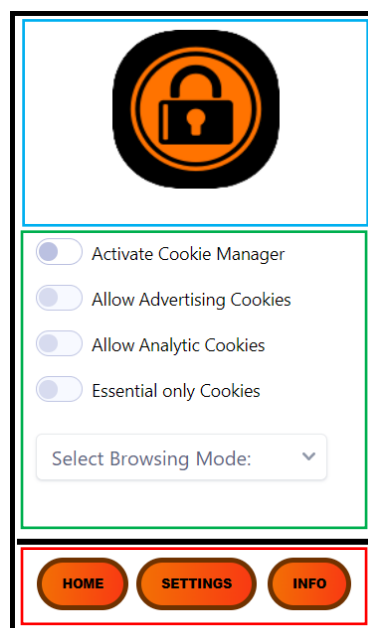

Figure 18 - Interface Popup Page

Figure 18 shows the initial popup page that is displayed to the user when they click the extension icon. The popup page is split into three main sections, the logo section highlighted in **blue,** and the taskbar section highlighted in **red** are static and remain in the same location regardless of the page the user is on. This was done to create uniformity and consistency in the design of the tool, the user selection

section highlighted in **green** allows the user to activate the tool, individually select their preferred cookies or select a browsing mode.
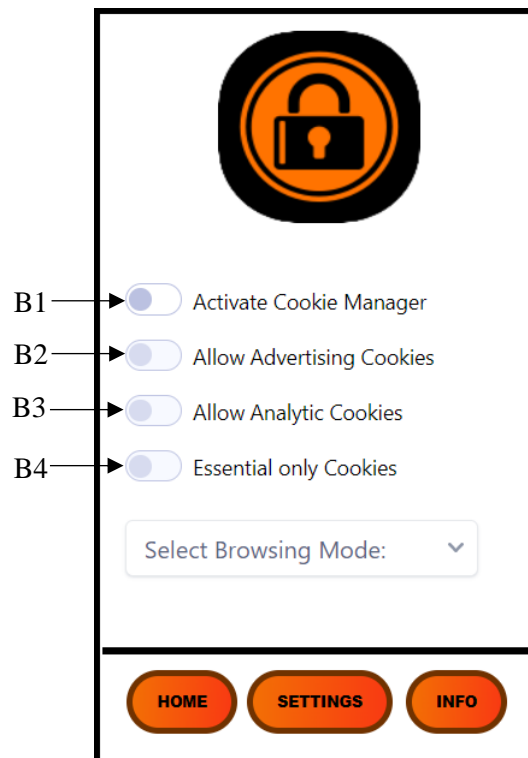

Figure 19 - Interface Button Selection

Once the tool has been activated using the 'Activate Cookie Manager' button (B1) the three cookie selection buttons (B2, B3, B4) are enabled, depending on the button selection by the user, certain buttons are disabled based on their last button selection (see figure 17).

The user can also choose to select a browsing mode rather than individually selecting the type of cookies they allow. There are three browsing modes:

1. Max Privacy Mode
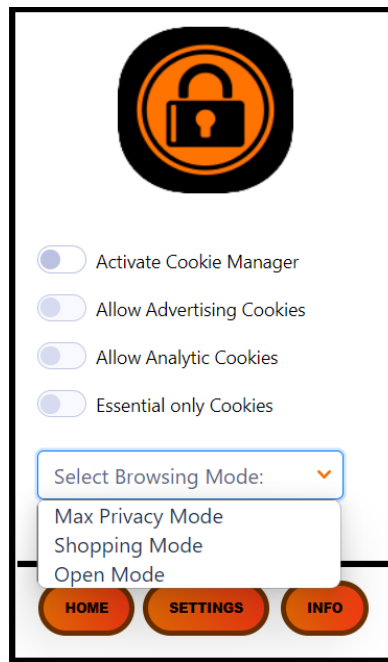
2. Shopping Mode

3. Open Mode

Figure 20 - Interface Browsing Mode Selection

Each browsing mode allows a certain variation of the three cookie types shown above:

1. Max Privacy Mode

    a. Allows Essential Cookies only

2. Shopping Mode

    a. Allows Advertising Cookies only

3. Open Mode

    a. Allows Advertising Cookies

    b. Allows Analytic Cookies

Once the user has made their cookie selection the interface can be closed, and the tool functions based on the user's selection until it is changed, or the tool is deactivated.

4.6.2 Settings Interface

The settings page is designed to allow the user to effortlessly switch between an interface theme and also blacklist and whitelist a URL, achieving requirements FR3, FR4, FR5, FR6 and FR12.
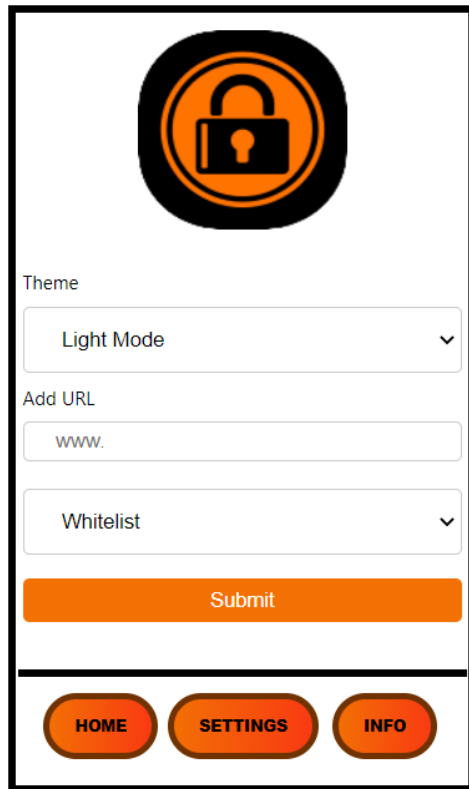
Figure 22 - Interface Setting Page
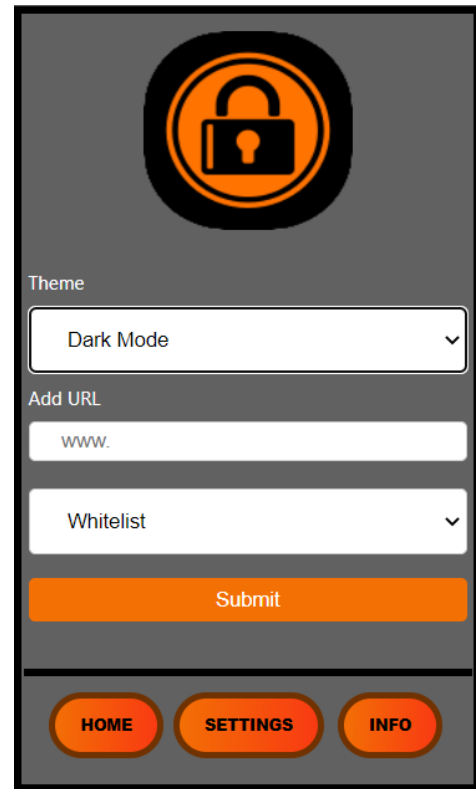
Figure 21 - Interface Setting Dark Mode

The settings page interface allows the user to switch between the default light theme and a dark theme, once the theme is set the tools interface transitions to display the new theme. The theme setting is stored using local storage and is applied to all pages of the interface until the theme is changed or the extension is deleted and reinstalled. Satisfying requirement FR6.

The settings page also introduces the user to the whitelist/blacklist functionality. This feature allows the user to add a URL to the input form and then select using the drop-down menu if they would like to whitelist or blacklist the entered URL. The list can be deleted by clearing the tools local storage. Satisfying requirements FR3, FR4, FR5 and FR12.

The list is created when the first entry is entered by the user, two separate lists are used:

1. Whitelist
2. Blacklist

The whitelist stores the URL entered by the user, if the URL stored in the list matches the current users URL of the user's browser the tool will override the user's current cookie selection and accept all cookies for that URL. The blacklist functions the same as the whitelist except it will override the user's current selection and enter 'Max Privacy Mode' only allowing essential cookies that the website needs to function. The lists are stored until the user deletes the entire list or the extension is deleted and reinstalled.

4.6.3 Information Interface

The interfaces information page educates the user on the purpose of different types of cookies that the tool affects. This achieves requirement NFR3 and is implemented with the project's education objective in mind.
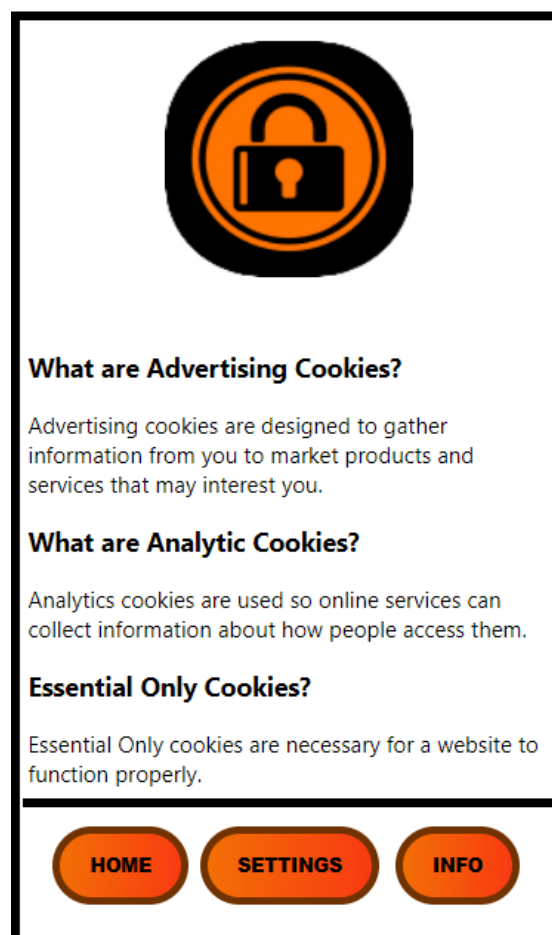

Figure 23 - Interface Info Page

Chapter 5 Evaluation

5.1 Overview

This chapter covers the evaluation of the tool. Evaluation is separated into two main sections, firstly section 5.3 will cover the technical evaluation of the tool and section 5.4 will cover the usability evaluation.

5.2 Evaluation Strategy

The tools technical evaluation is primarily focused on programmable testing, this involves both general and task specific testing. Testing took place after each development iteration with four testing periods during the project's timeline, continuous testing was also used throughout the project.
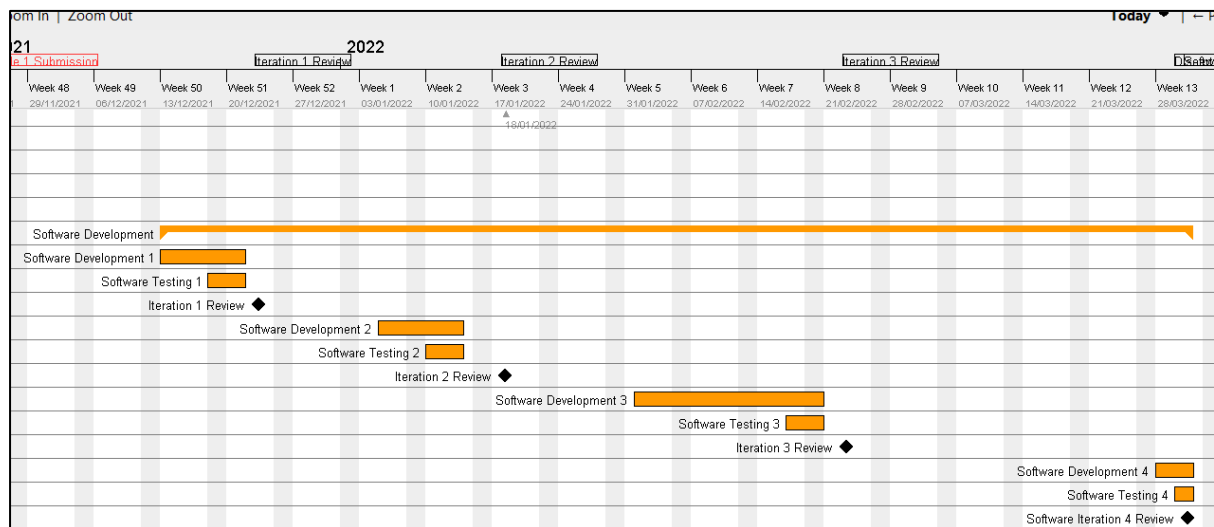

Figure 24 - Project Testing & Development Timeline

The useability evaluation covers the tools useability, this involves participants evaluating the tools interface useability and experience. The interface evaluation took place during the planned study period, this involved some participants recording their screens while they completed a number of set tasks (see Section 5.5.2). Various metrics were measured during this evaluation which will be discussed further in Section 5.4. Participants were also presented with a useability questionnaire after they had completed the set tasks.

5.3 Technical Evaluation

The technical evaluation involved two main aspects, firstly a test environment (TE1) was created using the MACS student homepage, this was used to test script injection and ensure the tool could access elements of a webpage that was designed specifically for its use. Once the minimum functionality has been achieved, a second test environment (TE2) was used (wordpress.com) to test the remaining elements needed to meet the requirements stated in Chapter 3. Wordpress.com was chosen due to its large audience and its use of standard naming conventions.

5.3.1 Accessing Elements Evaluation

One of the main obstacles to overcome with the tool is being able to access an element on a webpage that was created by another developer, to overcome this initial hurtle a test environment containing a single webpage was used. The webpage contained a single button and checkbox, with the elements ids and classes known it eliminated the need to use other development tools to find them. This allowed the focus to be on injecting a script into the webpage and simulating a mouse click as shown in Section 4.5.

After it was determined that the tool could successfully inject a script and simulate a mouse click it was necessary to test the functionality in a real-world scenario. Using a webpage created by another developer introduces an array of new obstacles, firstly the classes and ids of the page's elements are now unknown, unlike the previous test environment. The pages elements are also layered onto a cookie banner and thus must be referenced in the correct order, another complexity involves executing commands in the correct sequence as a human would when viewing a cookie banner.
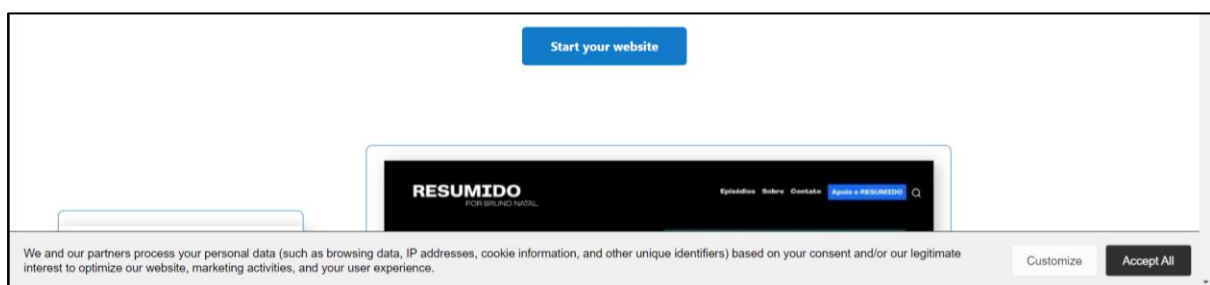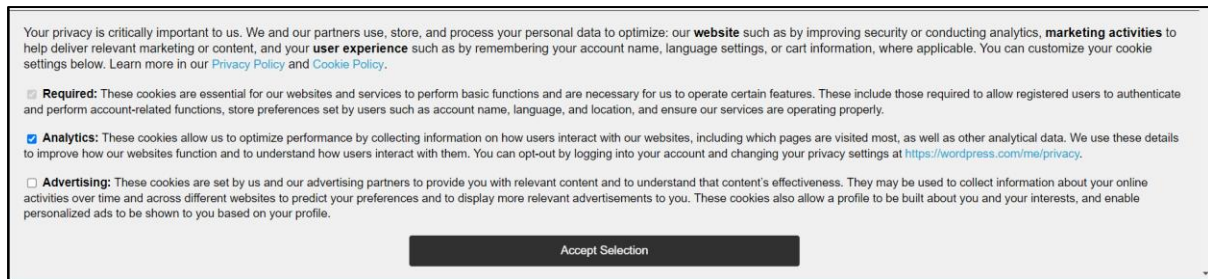

Figure 25 - Test Environment 2 (TE2) Cookie Banner

Figure 26 - Test Environment 2 (TE2) Cookie Banner Expanded

Chrome DevTools was a key part of the second test environment, query selectors were used to access the elements on the cookie banner, as detailed in Section 4.5.2. Delay functions were used to verify the script was clicking the elements in the correct order as a normal script injection happens too fast for the human eye to verify. Colour coding was also used to ensure the correct elements had been selected with all buttons and checkboxes set to red initially, then turned to green once they had been clicked. The delay functions coupled with colour coding allowed for extensive verification that the correct element had been selected in the correct sequence.

The figures below show the output of visually verifying that the tool has selected the correct element in the desired sequence.

Figure 27 - TE2 before Tool Selection
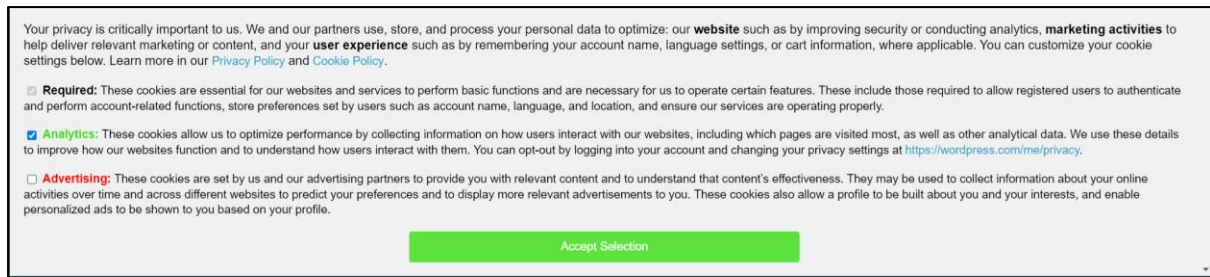
Figure 28 - TE2 after Tool Selection

5.3.2 Cookie Selection Evaluation

Initially TE2 was used to check the tool was selecting the correct elements of a cookie banner by manually sorting through the saved cookies for that webpage using Chrome DevTools. Three test scenarios were used:

1. Accept all cookies

2. Accept advertising cookies only

3. Accept essential cookies only

With each test scenario there are two separate run throughs, firstly all cookies are cleared, and the tool is disabled, the options are then selected on the cookie banner manually, Chrome DevTools is then used to save the list of cookies that are produced after the banner selection. In the second run through the cookies are cleared and the tool is enabled with the same selection that was followed in the first run through, again Chrome DevTools is used to save the list of cookies that are produced. The two lists are then checked to ensure they are the exact same, if the lists match this is indication that the cookies produced by the tool's selection are the same as the human's selection, indicating that the feature has operated correctly. This simulation was run for each of the test scenarios, for a total of six run throughs.

Figure 29 - Example Cookie List

While performing this testing it was noted that the webpage may produce extra cookies that did not follow the selection made on the cookie banner, this introduced additional data into the lists and thus they did not match. As this is outside of the scope of the project, it was decided that the other method of testing discussed in section 5.3.1 was more suitable.

5.3.3 Local Storage Flags Evaluation

Once it has been evaluated that the tool is able to handle cookie requests automatically based on the user's selection it is necessary to evaluate that the interface is correctly connected to the background scripts. As with the evaluation mentioned in section 5.3.1 and section 5.3.2 only required the use of background scripts it is essential to now test the tool using the user interface as the main selection point. Local storage flags were used to keep track of the user's selection on the interface, once the user makes their preferred cookie selection the accompanying flag is set to active in the background script. The testing simulation discussed in section 5.3.1 using TE2 was then re-run with the tools interface being used to select the preferred cookies rather than hard coding in the background script. All cookie selection possibilities were tested as follows:

1. Essential cookies only

41

2. Advertising cookies only

3. Analytic cookies only

4. Max privacy mode (browsing mode selection)

5. Shopping mode (browsing mode selection)

6. Open mode (browsing mode selection)

After successful tests of all six browsing scenarios, it was determined that the user interface was correctly connected to the background scripts.

5.4 Useability Evaluation

The useability evaluation covers the tools user experience and useability. The system being evaluated is the tools interface (shown in Section 4.6). The aim of the interface is to be clear and intuitive to navigate and operate without any prior knowledge of Chrome extensions or cookie managers. In addition to the tool being user friendly (meeting the **Useability** objective) it should also be privacy friendly and educate its users on the purpose of different types of cookies (meeting the **Informed Decisions** and **Education** objective).

The online research study poses three sections, firstly a demographics questionnaire collecting information on the participants current browsing habits and experience with browser extensions. The first section also collects information on the participants level of knowledge regarding cookies, this helps to measure the level of depth needed regarding the **Education** objective.

Section two features several working tasks that gives the participant an opportunity to navigate and operate the tools interface. A number of participants are asked to record their screens during this section to collect information on the order and time taken to complete some of the tasks requiring more problem solving. Section three contains a useability questionnaire asking the participant various useability focused questions using a Likert scale on their experience with the tool.

The full research study is included in Appendix A.

5.5 Evaluation Results

The study was hosted fully online with participants evaluating *only* the tools interface as downloading and installing the tool to their browser posed a multitude of ethical barriers.

The full processed anonymised study results are included in Appendix B.

5.5.1 Demographics

There were 6 participants that took part in the study with the overwhelming majority in the 18 to 24 years old age range. One participant was in the 25-30 age range. This age range was as expected as the study was conducted using Heriot Watt University students. Although the number of participants is lower than the initially scheduled 10 participants due to complications regarding Covid-19, the dataset still represents a wide variation in skill level and demographics.
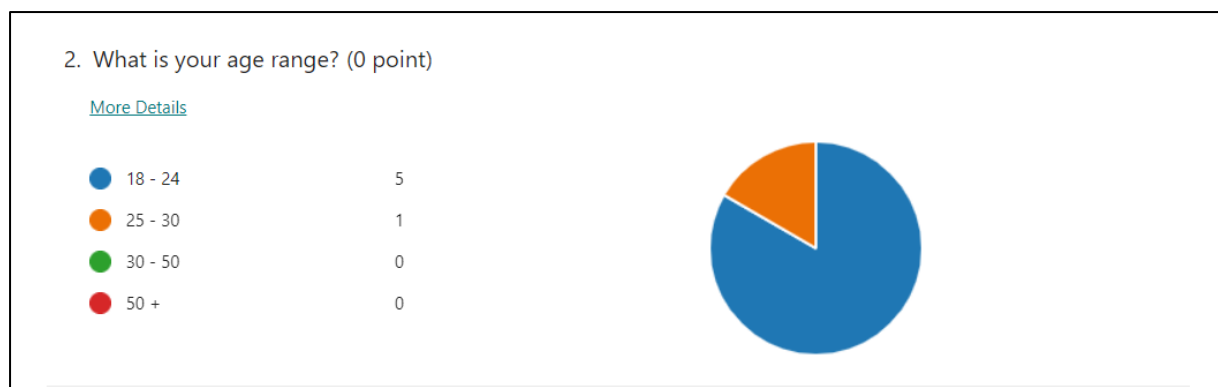
Figure 30 – Age of participants

The most commonly used browser was Google Chrome and over 83% of participants spend a large portion of their day browsing the web, this is a good sample group as the participants spending a large portion of their day browsing the web are more likely to interact with cookie banners.

3. How many hours do you spend browsing the web per day ? (0 point)

More Details

- < 1   0
- 1- 2   1
- 3 - 4   3
- 5 +   2
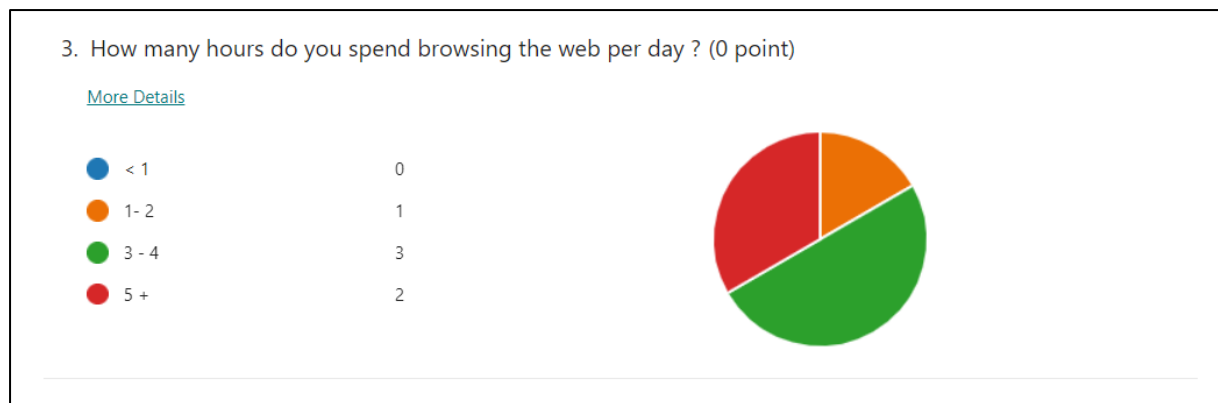
Figure 31 - Number of hours spent browsing per day

The participants were asked for their usual response to a cookie banner. The answer options were:

1. Accept all cookies

2. Reject all cookies

3. Adjust accepted cookies to my personal preferences

4. Ignore the cookie banner and continue browsing

67% responded they usually accept all cookies as it is the easiest and quickest option. This is the exact target audience for the tool and will give a good insight into if the tool can make a user's interaction with cookie banners more user friendly.

7. When a website displays a cookie banner I usually... (0 point)

More Details

- Accept all cookies   4
- Reject all cookies   1
- Adjust accepted cookies to my ...   1
- Ignore the cookie banner and c...   0
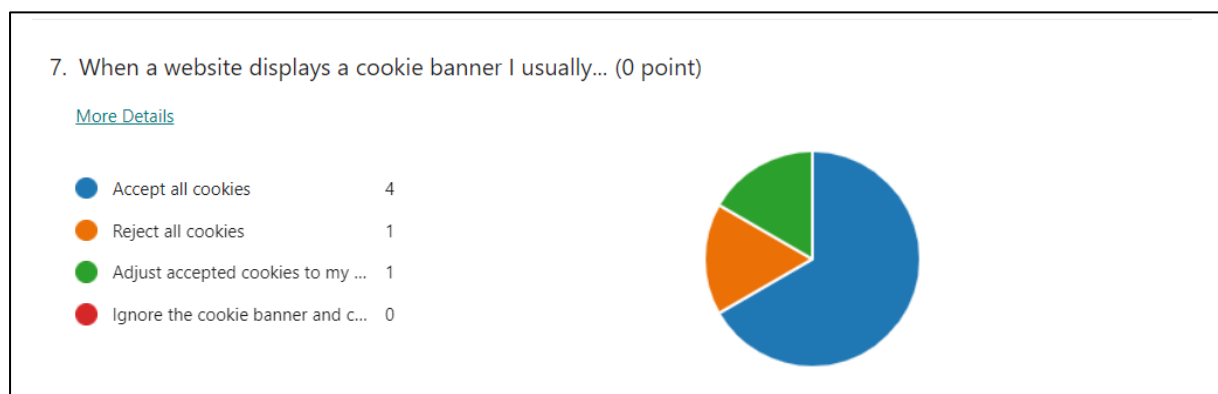
Figure 32 - Participants browsing habits

44

In order to gauge the participants general priorities when browsing the web, they were asked whether they value privacy or ease of use when using a website. Most participants value them an equal amount with no participants stating they value ease of use exclusively. This will most likely lead to good feedback from the participants as it will show if the tool is capable of helping the users increase their privacy online while still allowing websites to remain easy to use.
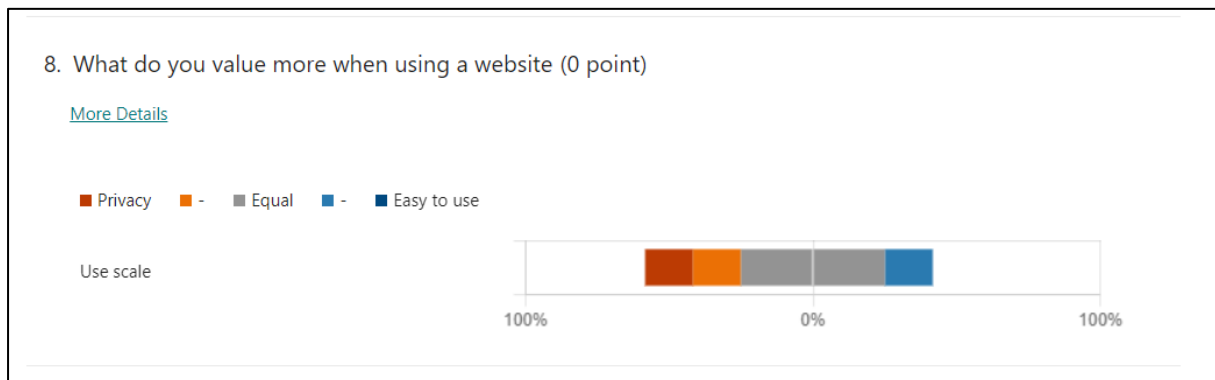
Figure 33 - Participants value when browsing

Finally, the participants were asked how familiar they are with both cookies and browser extensions. There was a wide range of responses regarding familiarity with browser extensions, this will give a good insight into the tool's useability for all skill levels. The participants also gave a wide range of responses regarding their knowledge of browser cookies, again this is useful to see the response to the tools education objective with each participant starting at a different knowledge level.

5.5.2 Working Tasks Results

The participants were asked to complete 9 different tasks using the tool. The tasks were designed to navigate the participant around the whole tool and allow them to interact with all of the main features, the tasks had a varying level of difficultly with the later tasks being more challenging than the first. All participants completed the 9 tasks with 3 participants recording their screens during this section, this allowed for a better insight into the process the participant took in order to complete the task and also the time it took them. All participants began from the same starting point (popup page) and were asked to complete the task in the order they were presented.

A full list of the tasks can be found in [Appendix B](#).

5.5.2.1 Cookie Protection Level

This task instructed the participant to change their browsing mode to the highest protection level. The task was completed by navigating to the 'Select Browsing Mode:' drop down menu and selecting 'Max Privacy Mode'. All participants completed this task successfully with the screen recorded participants taking less than 3 seconds to complete the task. This shows the home page of the tool is very clear visually, indicated by the short amount of time it took to find the 'Select Browsing Mode:' drop-down. In a poorly designed and cluttered page you would expect to see a long time to complete the task. The home page is also easy to navigate, shown by all participants completing the task with ease.

5.5.2.2 Dark/Light Theme

This task instructed the participants to change the tools' theme from the default light theme to dark. The task was completed by navigating using the taskbar to the settings page and selecting 'Dark Mode' from the theme drop down menu. All the participants completed the task successfully with the screen recorded participants navigating straight to the settings page without clicking anywhere else. As all participants completed the task with ease it can be said that navigating the tools layout is intuitive as the participants found the settings page straight away without searching elsewhere.

5.5.2.3 Disabled Features

This task instructed the participants to *try* to turn on essential cookies using the slider buttons on the homepage. The task was completed by navigating back to the home page using the task bar and selecting the 'Essential Only Cookies' slider, however as the browsing mode had already been set previously the tool does not allow you to use the 'Essential Only Cookies' button as it is disabled. This task was designed to identify how the user interacts with the individual buttons after a browsing mode has already been set. All participants completed this task however 2 participants needed additional instructions to re-read the task careful as they had not understood that they were only to *try* and turn on 'Essential Only Cookies'. Although this task did not give an insight into the tools current design it gave valuable information on a user's thought process which can be used in later versions of the tool.

5.5.2.4 Blacklist 'www.google.com'

This task instructed the participants to add the URL 'www.google.com' to their blacklist. Blacklisting a site causes the tool to automatically enter 'Max Privacy Mode' (see section 4.6.1). The task was completed by navigating to the tool's settings page and entering the URL into 'Add URL' text input box, the user then selects 'blacklist' from the drop-down menu and clicks the 'Submit' button. The 'Submit' button then turns green as confirmation the URL has been added. All of the participants completed the task however 3 of them asked what effect blacklisting a URL would have for the tool. As all of the participants successfully navigated and completed the task it is clear that this feature is intuitive, however as 3 of the participants needed additional information to understand the feature it is noted that this particular action could be improved with a user prompt explaining its effects.

5.5.2.5 Education

This task followed a different format from the others and instructed the user to use the tool in order to find out information regarding cookies. The participant's task was to find out what essential only cookies are. The task can be completed by using the task bar to navigate to the information page of the tool, the participant is then presented with the information on different types of cookies. This task had a 100% success rate with all participants navigating straight to the page and completing the task without additional help. As all participants were able to quickly navigate to the correct page and learn information on cookies this task was successful in showing the tools design in consistent, clear and informative.

5.5.2.6 Feature Activation

The final task involved instructing the participants to complete a set number of tasks in a specific order. The participants were asked to activate the cookie manager, enable essential only cookies and then enable advertising cookies. This task can be completed in multiple different ways with the objective of the task being to find out the most user-friendly way of completing the task in the least number of steps. When essential only cookies are selected all other cookie selection options are disabled, as essential only categorisation does not include advertising or analytical cookies. The most popular method of

completing this task was to disable essential only cookies and then re-select advertising cookies, however 2 of the participants needed additional help to complete the task. It was noted that the user interface should include prompts to the user if they have unsuccessfully selected a disabled feature multiple times. This task was crucial in improving the interfaces useability for a novice user and gave additional features to be added in the post study changes.

5.5.3 Useability Questionnaire Results

The final section of the study asked the participants to complete 8 useability questions regarding their experience using the tools interface. The final section also included an area for the participants to express any other comments they had regarding the tool.
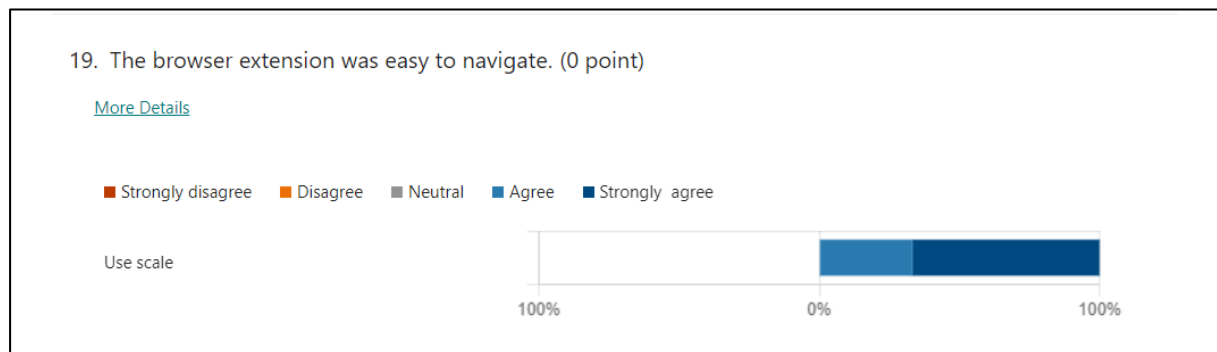
Figure 34 - Participants opinion on the tool's navigation

As shown in the above figure all participants agreed or strongly agreed that they found the tool easy to navigate. Although this is a positive result regarding the tools navigate it is noted that 2 of the participants did not strongly agree, this is most likely due to the confusion caused during the final task with 2 participants needing additional help to complete the task. 1 participant also noted that the 'disabled buttons' were confusing, this has been recorded and will be addressed in the post study changes (see section 5.6).
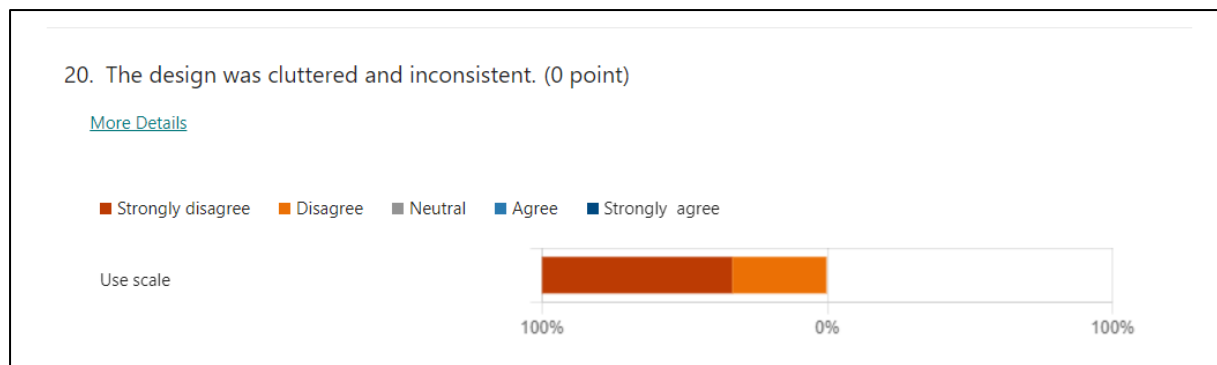
Figure 35 - Participants opinion on the tool's design

The above figure shows clear disagreement towards the statement "The design was cluttered and inconsistent". This again is a positive result that can be further supported by the participants ability to successfully navigate around the tool and select features quickly and instinctively.
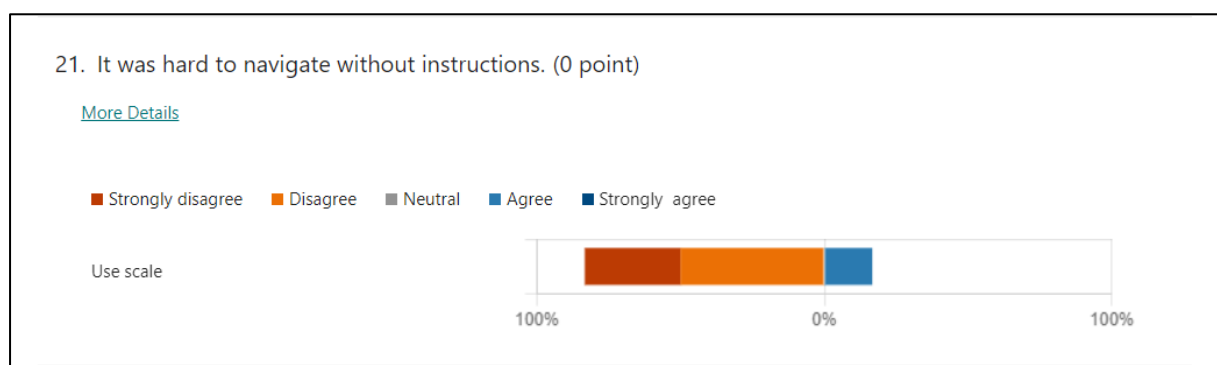
Figure 36 - Participants opinion on tool's navigation without instructions

The above figure shows the most variation in opinions regarding the tool needing instructions. Although the majority of participants said they either disagree or strongly disagree that the tool was hard to navigate without instructions 1 participant agreed. This can be explained by the additional helped needed in completing the final working task, it has been recorded that the tool would benefit from additional instructions in the form of user prompts when a user has unsuccessfully selected a disabled feature multiple times.

All participants stated that they would recommend the tool to other people and when asked to give any additional comments, 1 of the participants suggested the tool would benefit from additional information regarding the tools black/whitelist feature and another noted that the disabled buttons needed

supplementary instructions. These comments have been noted and have been addressed in the post study changed.

5.6 Post Study Changes

The useability study provided lots of information on changes that would improve the tools overall useability and subsequently improve the user experience. The participants were also asked to leave additional comments regarding the tool, these comments can be categorised into two main areas. Firstly, it was noted that more information was required for them to understand the blacklist/whitelist feature and additional instructions were required to stop users attempting to select disabled buttons. The first issue was addressed by adding information to the settings page describing the effect blacklisting or whitelisting a URL will have on the tool. The second comment was addressed by adding in a user prompt if a user has clicked a disabled feature multiple time.

5.7 Requirements Summary

The following shows a summary and details the status of requirements set out at the start of the project in Chapter 3.

The following table summarises the status of the project's functional requirements.

ID	Comment	Status
FR1	This was a **must** have requirement that was completed towards the start of the project. Section 4.6.1 details its implementation.	Complete
FR2	This was a **must** have requirement that was completed at the start of the project. Section 4.5.3 details its implementation.	Complete
FR3	This was a **could** have requirement that was completed using lists. Section 4.6.2 details its implementation	Complete
FR4	This was a **could** have requirement that was completed using lists. Section 4.6.2 details its implementation	Complete
FR5	This was a **could** have requirement that was completed. See section 4.6.2.	Complete

FR6	This was a **should** have requirement that was completed using an input form. Section 4.6.2 details its implementation	Complete
FR7	This requirement was initially attempted however it was found to be outside of the scope of the project as the tool does not directly interact with the cookies themselves.	Incomplete
FR8	This was a **must** have requirement that was completed towards the start of the project. Section 4.6.1 details its implementation.	Complete
FR9	This requirement was initially attempted however it was found to be outside of the scope of the project as the tool does not directly interact with the cookies themselves.	Incomplete
FR10	This was a **could** have requirement that was completed after initial functionality was added. Section 4.6.1 details its implementation.	Complete
FR11	This requirement was not attempted due to it being outside of the scope of the project as the tool does not directly interact with the cookies themselves.	Incomplete
FR12	This was a **could** have requirement that was completed due to the nature of the whitelist/blacklist feature using local storage. Section 4.6.2 details its implementation.	Complete

Table 4 - Completed Functional Requirements Summary

The following table summarises the status of the projects non-functional requirements.

ID	Priority	Status
NFR1	The tool was developed using the Chrome API and Chrome DevTools. Section 4.4.1 details the tools development.	Complete
NFR2	It was concluded by the useability study that the tool was simple to navigate. See section 5.5.3 for full evaluation.	Complete
NFR3	The tools information page educates the user on different types of cookies the tool can select. Section 4.6.3 details its implementation.	Complete

| NFR4 | The tool was not found to greatly increase browser loading times. This was evaluated throughout testing. See section 5.3 | Complete |
| NFR5 | The tool does not directly access the user's data and instead manipulates cookie banners on the websites the user visits. The tool also informs users of the effects changing the tools settings will have. | Complete |

Table 5 - Completed Non-Functional Requirements Summary

The tool completed rigorous testing and evaluation throughout the course of the project. The technical evaluation provided a basis to ensure the tool met the function requirements laid out in Section 3.2 with the main focus on guaranteeing the tool could receive a selection from the user and automatically manage their cookie interactions on a web page. The useability evaluation provided excellent feedback on improvements that could be made to the tool as well as verifying the tools interface was intuitive, easy to use and most importantly satisfying the tool met its **aim** of being user friendly as described in section 1.2.

Chapter 6 Conclusion

6.1 Overview

The aim of the project was to build a user and privacy friendly tool that automatically deals with a user's cookie interactions while web browsing. With privacy and useability being clear project objectives, it was important to ensure the tool provided the user with both. The projects focal point was not to just build on current useable security but to improve the user's interaction with cookies on a webpage, this was done by educating and informing the user on the consequences of the cookie selection they have chosen. It was also decided that the tool must be fully GDPR compliant, and this was achieved by making sure the tool did not interact or directly access the user's personal data.

Current solutions were showcased as well as highlighting that they are insufficient in meeting the objectives of this project. The tool was implemented following the requirements set out at the beginning of the project as well as keeping the projects aims and objectives in mind. The tool was then rigorously evaluated both technically, with iterative rounds of testing as well as being evaluated by participants in a useability research study. Testing showed the tool met almost all of its originally set requirements, along with the research study concluding it was easy to use, privacy friendly and most importantly achieved the goal of improving the user's interaction with cookies.

6.2 Limitations & Future Work

The scope of this project is vast and can be extended to incorporate a range of additional features, as the web grows, and cookies continue to become more invasive and data consuming there are two main extensions that can be added to improve both useability and privacy.

6.2.1 Data Set

The projects current main limitation is the number of web pages that it can successfully function on, due to the lack of standard naming conventions in web development, the ids and class names for elements on a cookie banner follow no standard format and are chosen purely by the developer. This

means the majority of websites have different element ids that the tool cannot query select, an exception to this is websites built using a website builder such as wordpress.com, that follow standard automatic naming conventions. In order to increase the number of webpage that the tool can function on a data set needs to be created and categorised. There are two ways to achieve this, firstly you could crowd source the data asking a large number of users to manually identify the element ids and classes for each cookie banner they encounter, by categorising this data, a data set will be built with the correct naming conventions and corresponding URL's. This would allow the tool to search its data set for the correct element ids and classes when it encounters a new page it has not interacted with before. The second way to achieve this data set is to build web scraper bot that extracts the underlying html code from each webpage it visits and categories the elements on the cookie banner into standard naming conventions compatible with the tool.

6.2.2 Webpage Accountability

Currently the tool interacts with a webpages cookie banner and does not directly interact with the cookies themselves. Although it is out of the scope of this project there is lots of literature on the topic of webpages not following the user's cookie selection. An example of this is a webpage continuing to use advertising cookies even after the user has selected to reject them. At present there is no way for a user to easily know if a webpage is following their selection, one way to extend the tools privacy aspect, is to begin to record the cookies that the webpage uses, the tool can then search this data and alert the user if the webpage that they are currently on is **not** following their chosen selection. This expands upon the tool's privacy aim and GDPR compliance objective by notifying the user when a webpage is breaking GDPR regulations.

6.2.3 Cookie Deletion

As aforementioned the tool does not directly interact with a user's cookies, another way to expand the tools privacy is by developing a kill switch that clears a user's cookies at the end of a browsing session or when they leave a specific webpage. There are currently ways to clear your cookies through both other browser extensions and the web browser settings themselves, however adding this functionality

to the tool would allow the user to enjoy all of the current features as well as being able to categories URLs into privacy groups. The user could then select both the type of cookies they want to have cleared automatically and the webpages they want this action to be performed on.

6.2.4 Browser Expansion & Useability

Despite Google Chrome having the largest market share of web browsers, there are other web browsers that the tool could be made compatible with. There are also efforts that can be made to improve the tool useability, a more extensive useability study could be conducted with a larger number of participants. This data could then be used to increase the tools customisation with the addition of user profiles allowing the user more freedom and convenience, as currently the tools appearance, colour scheme and layout is the same for all users.

Chapter 7 References

[1] Hormozi, A.M. (2005) 'Cookies and Privacy', *Information Systems Security*, 13(6), pp. 51–59.

[2] Voigt, P. and von dem Bussche, A. (2017) 'Introduction and "Checklist"', in Voigt, P. and von dem Bussche, A. (eds) *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham: Springer International Publishing, pp. 1–7. doi:10.1007/978-3-319-57959-7_1.

[3] 'Art. 7 GDPR – Conditions for consent' *General Data Protection Regulation (GDPR)*. Available at: https://gdpr-info.eu/art-7-gdpr/ (Accessed: 21 November 2021).

[4] 'Art. 5 GDPR – Principles relating to processing of personal data' (no date) *General Data Protection Regulation (GDPR)*. Available at: https://gdpr-info.eu/art-5-gdpr/ (Accessed: 21 November 2021).

[5] Utz, C. *et al.* (2019) '(Un)informed Consent: Studying GDPR Consent Notices in the Field', in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. New York, NY, USA: Association for Computing Machinery (CCS '19), pp. 973–990. doi:10.1145/3319535.3354212.

[6] Dabrowski, A. *et al.* (2019) 'Measuring Cookies and Web Privacy in a Post-GDPR World', in Choffnes, D. and Barcellos, M. (eds) *Passive and Active Measurement*. Cham: Springer International Publishing (Lecture Notes in Computer Science), pp. 258–270. doi:10.1007/978-3-030-15986-3_17.

[7] Sanchez-Rola, I. *et al.* (2019) 'Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control', in *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*. New York, NY, USA: Association for Computing Machinery (Asia CCS '19), pp. 340–351. doi:10.1145/3321705.3329806.

[8] Optout.networkadvertising.org. 2021. *NAI Consumer Opt Out*. [online] Available at: <https://optout.networkadvertising.org/?c=1> [Accessed 22 November 2021].

[9] TrustArc The Leader in Privacy Management Software. 2021. *TRUSTe Privacy Certification Standards*. [online] Available at: <https://trustarc.com/consumer-info/privacy-certification-standards/> [Accessed 22 November 2021].

[10] Darkpatterns.org. 2021. *Dark Patterns*. [online] Available at: <https://www.darkpatterns.org/> [Accessed 22 November 2021].

[11]   Chrome.google.com.   2021. *Vanilla   Cookie   Manager*.   [online]   Available   at: <https://chrome.google.com/webstore/detail/vanilla-cookie-manager/gieohaicffldbmiilohhggbidhephnjj?hl=en> [Accessed 22 November 2021].

[12] K.-P. Yee, "User Interaction Design for Secure Systems," Proc. 4th Int'l Conf. Information and Communications Security, Springer-Verlag, 2002, pp. 278–290.

[13] Payne, B.D. and Edwards, W.K. (2008) 'A Brief Introduction to Usable Security', *IEEE Internet Computing*, 12(3), pp. 13–21. doi:10.1109/MIC.2008.50.

[14] Zesty.ca. 2021. *Secure Interaction Design*. [online] Available at: <http://zesty.ca/sid/> [Accessed 22 November 2021].

[15] Javascript.com. 2022. *JavaScript.com*. [online] Available at: <https://www.javascript.com/> [Accessed 9 April 2022].

[16] Developer.mozilla.org. 2022. *HTML: HyperText Markup Language | MDN*. [online] Available at: <https://developer.mozilla.org/en-US/docs/Web/HTML> [Accessed 3 April 2022].

[17]   W3.org.   2022. *Cascading   Style   Sheets*.   [online]   Available   at: <https://www.w3.org/Style/CSS/Overview.en.html> [Accessed 27 March 2022].

[18] Code.visualstudio.com. 2022. *Visual Studio Code - Code Editing. Redefined*. [online] Available at: <https://code.visualstudio.com/> [Accessed 20 March 2022].

[19] Chrome Developers. 2022. *Chrome DevTools - Chrome Developers*. [online] Available at: <https://developer.chrome.com/docs/devtools/> [Accessed 27 February 2022].

[20] Park, J.S. and Sandhu, R. (2000) 'Secure cookies on the Web', *IEEE Internet Computing*, 4(4), pp. 36–44. doi:10.1109/4236.865085.

[21] Ico.org.uk. 2021. *How do we comply with the cookie rules?*. [online] Available at: <https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/> [Accessed 22 November 2021].

[22] The Guardian. 2021. *LA Times among US-based news sites blocking EU users due to GDPR*. [online] Available at: <https://www.theguardian.com/technology/2018/may/25/gdpr-us-based-news-websites-eu-internet-users-la-times> [Accessed 22 November 2021].

[23] En.wikipedia.org. 2021. *System usability scale - Wikipedia*. [online] Available at: <https://en.wikipedia.org/wiki/System_usability_scale> [Accessed 22 November 2021].

[24] Hu, X. and Sastry, N. (2019) 'Characterising Third Party Cookie Usage in the EU after GDPR', in *Proceedings of the 10th ACM Conference on Web Science*. New York, NY, USA: Association for Computing Machinery (WebSci '19), pp. 137–141. doi:10.1145/3292522.3326039.

[25] Rathod, D., 2017. Web browser forensics: google chrome. *International Journal of Advanced Research in Computer Science*, *8*(7), pp.896-899.

[26] Chrome Developers. 2022. *API Reference - Chrome Developers*. [online] Available at: <https://developer.chrome.com/docs/extensions/reference/> [Accessed 21 February 2022].

Appendix A Useability Study

Below is the full useability study the participants received, including the consent form.

Consent Form ⠙

* Required

Section 1 - Participant Details

1. Full Name *

2. Heriot Watt Email *

27/04/2022, 15:57   Consent Form

Section 2 - Consent

The purpose of this study is to evaluate the user interface of the given browser extension.

This is an online-only study, an internet connection and web browser are all that is required. Collected information will be stored securely and safely according to GDPR guidelines. Participation will have no effect on your marks for any subject at this, or any other university.

You may decline to participate and can withdraw at any time. If you choose to withdraw during the survey simply close your browser window.

If you do choose to withdraw any data already recorded will be deleted. Please send withdrawal requests to the email listed below.

<cf51@hw.ac.uk>

You must be at least 18 years of age and a current student of Heriot Watt University to participate in this

3. Date *

Please input date (dd/MM/yyyy) 🔲

4. Signature *
Please type your name in <BLOCK CAPITALS>

5. I have read and understood the consent form. *

◯ Consent

This content is neither created nor endorsed by Microsoft. The data you submit will be sent to the form owner.

 Microsoft Forms

https://forms.office.com/Pages/DesignPageV2.aspx?origin=NeoPortalPage&subpage=design&id=8I9CbGVo30Kk245q9jSBPS72sVGkEaINqCKv...   2/2

Cookie Manager Research Study

* Required

Section 1 - Consent Form

The purpose of this study is to evaluate the user interface of the given browser extension.

This is an online-only study, an internet connection and web browser are all that is required. Collected information will be stored securely and safely according to GDPR guidelines. Participation will have no effect on your marks for any subject at this, or any other university.

You may decline to participate and can withdraw at any time. If you choose to withdraw during the survey simply close your browser window.

If you do choose to withdraw any data already recorded will be deleted. Please send withdrawal requests to the email listed below.

<cf51@hw.ac.uk>

You must be at least 18 years of age and a current student of Heriot Watt University to participate in this

1. I have completed the consent form given. *

  ◯ Consent

Section 2 - Demographics

Please answer all questions

2. What is your age range? *

- ◯ 18 - 24
- ◯ 25 - 30
- ◯ 30 - 50
- ◯ 50 +

3. How many hours do you spend browsing the web per day ? *

- ◯ < 1
- ◯ 1- 2
- ◯ 3 - 4
- ◯ 5 +

4. How familiar are you with browser extensions? *

	Not Familiar	Slightly	Somewhat	Moderately	Extremely
Use scale	◯	◯	◯	◯	◯

62

5. What is your main web browser? *

○ Google Chrome

○ Microsoft Edge

○ Duck Duck Go

○ Tor

○ Firefox

○ Safari

○ Avast

○ Other

6. What is your level of knowledge regarding web browser cookies? *

	Beginner	Novice	Intermediate	Advanced	Expert
Use scale	○	○	○	○	○

7. When a website displays a cookie banner I usually... *

○ Accept all cookies

○ Reject all cookies

○ Adjust accepted cookies to my personal preferences

○ Ignore the cookie banner and continue browsing

27/04/2022, 16:05   Cookie Manager Research Study

8. What do you value more when using a website *

	Privacy	-	Equal	-	Easy to use
Use scale	○	○	○	○	○

9. Which statement best describes your web browsing habits *

☐ I don't like that websites track me using cookies.

☐ I like when websites recommend me ads based on my browsing history.

☐ I like when websites remember my passwords for me.

☐ I like when a website auto-completes information for me.

☐ None of the above.

Section 3 - Working Tasks

Please complete these task while using *only* the browser extension.

** This is a prototype study, some features may not function as intended **

10. Tool activation *

Please activate the cookie manager tool.

○ Completed.

○ Not completed.

11. Cookie Protection Level *

Please change your browsing mode to the highest protection level.

○ Completed.

○ Not completed.

12. Dark/Light Theme *

Please change the theme to dark mode.

○ Completed.

○ Not completed.

13. Dark/Light Theme *

Please change the theme back to light mode.

○ Completed.

○ Not completed.

14. Browsing Mode *

Please change your browsing mode to 'Shopping'.

○ Completed.

○ Not completed.

15. Disabled Features *

Please try to turn on essential only cookies.

○ Completed.

○ Not completed.

16. Black List *

Please add "www.google.com" to your blacklist

○ Completed.

○ Not completed.

17. Education *

Can you find out what 'Essential Only' cookies are?

○ Completed.

○ Not completed.

18. Feature Activation *

Please follow these steps in order.

1 - Activate cookie manager.
2 - Enable essential only cookies.
3 - Enable advertising cookies.

○ Completed.

○ Not completed.

Section 4 - Usability

Please complete the following questions after you have finished the tasks in section 3.

19. The browser extension was easy to navigate. *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Use scale	○	○	○	○	○

20. The design was cluttered and inconsistent. *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Use scale	○	○	○	○	○

21. It was hard to navigate without instructions. *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Use scale	○	○	○	○	○

22. I would use this browser extension in the future. *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Use scale	○	○	○	○	○

23. I understood what the browser extension was doing. *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Use scale	◯	◯	◯	◯	◯

24. I found the features useful. *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Use scale	◯	◯	◯	◯	◯

25. There should have been more features in the extension. *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Use scale	◯	◯	◯	◯	◯

26. I would recommend this extension to other people. *

◯ Agree

◯ Disagree

27. Any other comments about the browser extension.

Appendix B Study Data

Below is the anonymised processed data from the useability study.

Cookie Manager Research Study

6	05:27	Active
Responses	Average time to complete	Status

1. I have completed the consent form given. (0 point)

- Consent   6

2. What is your age range? (0 point)

- 18 - 24   5
- 25 - 30   1
- 30 - 50   0
- 50 +   0

27/04/2022, 16:21   Cookie Manager Research Study

3. How many hours do you spend browsing the web per day ? (0 point)

🔵	< 1	0
🟠	1- 2	1
🟢	3 - 4	3
🔴	5 +	2

4. How familiar are you with browser extensions? (0 point)

■ Not Familiar   ■ Slightly   ■ Somewhat   ■ Moderately   ■ Extremely

Use scale

100%   0%

5. What is your main web browser? (0 point)

🔵	Google Chrome	4
🟠	Microsoft Edge	0
🟢	Duck Duck Go	0
🔴	Tor	0
🟣	Firefox	0
🟤	Safari	2
🟣	Avast	0
⚪	Other	0

6. What is your level of knowledge regarding web browser cookies? (0 point)

■ Beginner   ■ Novice   ■ Intermediate   ■ Advanced   ■ Expert

Use scale

100%   0%

https://forms.office.com/Pages/DesignPageV2.aspx?origin=NeoPortalPage&subpage=design&id=8I9CbGVo30Kk245q9jSBPS72sVGkEalNqCKv...   2/8

27/04/2022, 16:21   Cookie Manager Research Study

7. When a website displays a cookie banner I usually... (0 point)

🔵	Accept all cookies	4
🟠	Reject all cookies	1
🟢	Adjust accepted cookies to my ...	1
🔴	Ignore the cookie banner and c...	0

8. What do you value more when using a website (0 point)

🟥 Privacy   🟧 -   ⬜ Equal   🟦 -   🟦 Easy to use

Use scale

100%   0%

9. Which statement best describes your web browsing habits (0 point)

🔵	I don't like that websites track ...	4
🟠	I like when websites recommen...	1
🟢	I like when websites remember ...	3
🔴	I like when a website auto-com...	2
🟣	None of the above.	1

10. Tool activation (0 point)

🔵	Completed.	6
🟠	Not completed.	0

https://forms.office.com/Pages/DesignPageV2.aspx?origin=NeoPortalPage&subpage=design&id=8I9CbGVo30Kk245q9jSBPS72sVGkEalNqCKv···   3/8

27/04/2022, 16:21   Cookie Manager Research Study

11. Cookie Protection Level (0 point)

● Completed.	6
● Not completed.	0

12. Dark/Light Theme (0 point)

● Completed.	6
● Not completed.	0

13. Dark/Light Theme (0 point)

● Completed.	6
● Not completed.	0

14. Browsing Mode (0 point)

● Completed.	6
● Not completed.	0

https://forms.office.com/Pages/DesignPageV2.aspx?origin=NeoPortalPage&subpage=design&id=8I9CbGVo30Kk245q9jSBPS72sVGkEalNqCKv-···   4/8

15. Disabled Features (0 point)

- ● Completed.   6
- ● Not completed.   0

16. Black List (0 point)

- ● Completed.   6
- ● Not completed.   0

17. Education (0 point)

- ● Completed.   6
- ● Not completed.   0

18. Feature Activation (0 point)

- ● Completed.   6
- ● Not completed.   0

19. The browser extension was easy to navigate. (0 point)

■ Strongly disagree   ■ Disagree   ■ Neutral   ■ Agree   ■ Strongly agree

Use scale

100%   0%

20. The design was cluttered and inconsistent. (0 point)

■ Strongly disagree   ■ Disagree   ■ Neutral   ■ Agree   ■ Strongly agree

Use scale

100%   0%

21. It was hard to navigate without instructions. (0 point)

■ Strongly disagree   ■ Disagree   ■ Neutral   ■ Agree   ■ Strongly agree

Use scale

100%   0%

22. I would use this browser extension in the future. (0 point)

■ Strongly disagree   ■ Disagree   ■ Neutral   ■ Agree   ■ Strongly agree

Use scale

100%   0%

27/04/2022, 16:21   Cookie Manager Research Study

23. I understood what the browser extension was doing. (0 point)

■ Strongly disagree   ■ Disagree   ■ Neutral   ■ Agree   ■ Strongly agree

Use scale

100%   0%

24. I found the features useful. (0 point)

■ Strongly disagree   ■ Disagree   ■ Neutral   ■ Agree   ■ Strongly agree

Use scale

100%   0%

25. There should have been more features in the extension. (0 point)

■ Strongly disagree   ■ Disagree   ■ Neutral   ■ Agree   ■ Strongly agree

Use scale

100%   0%

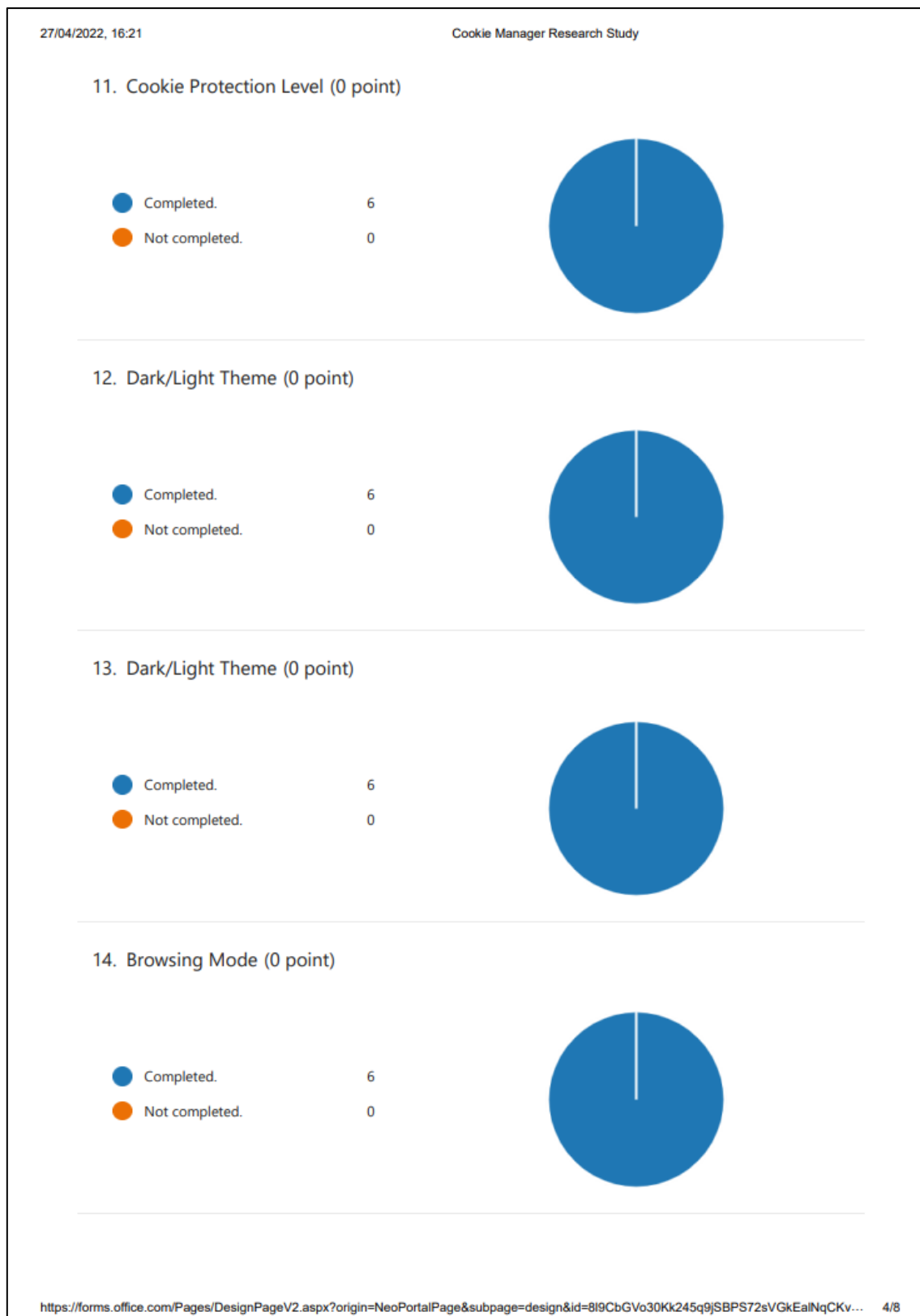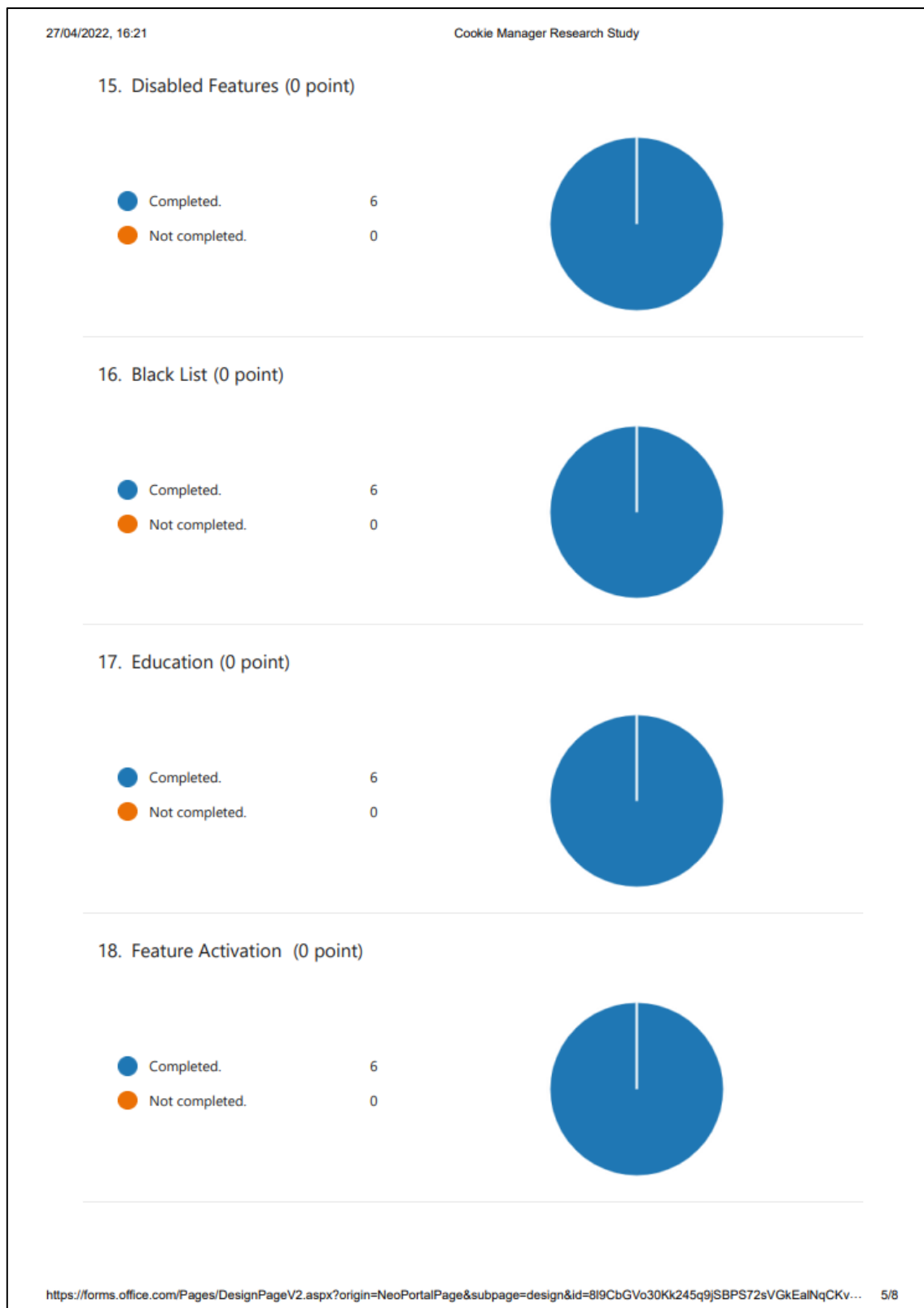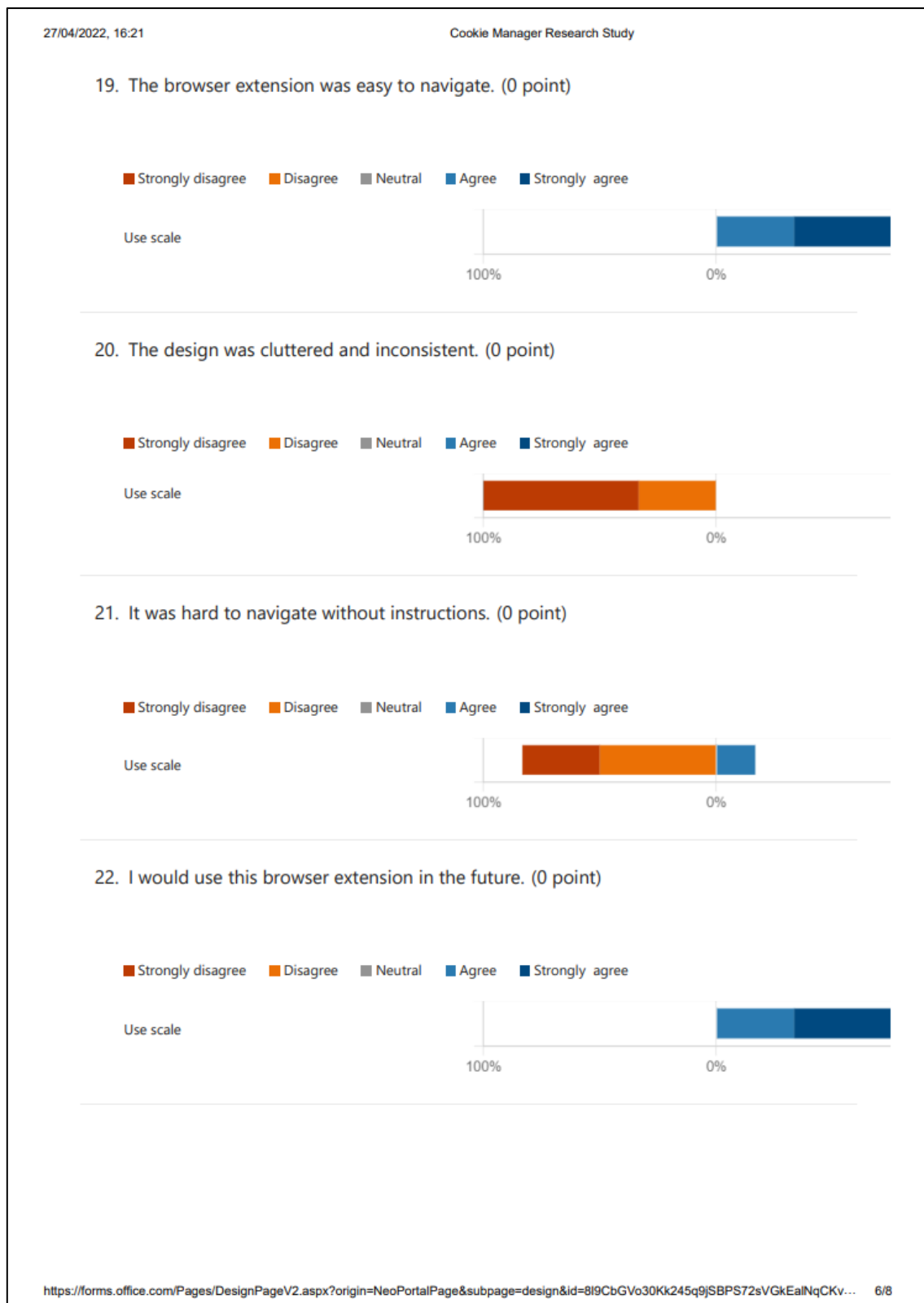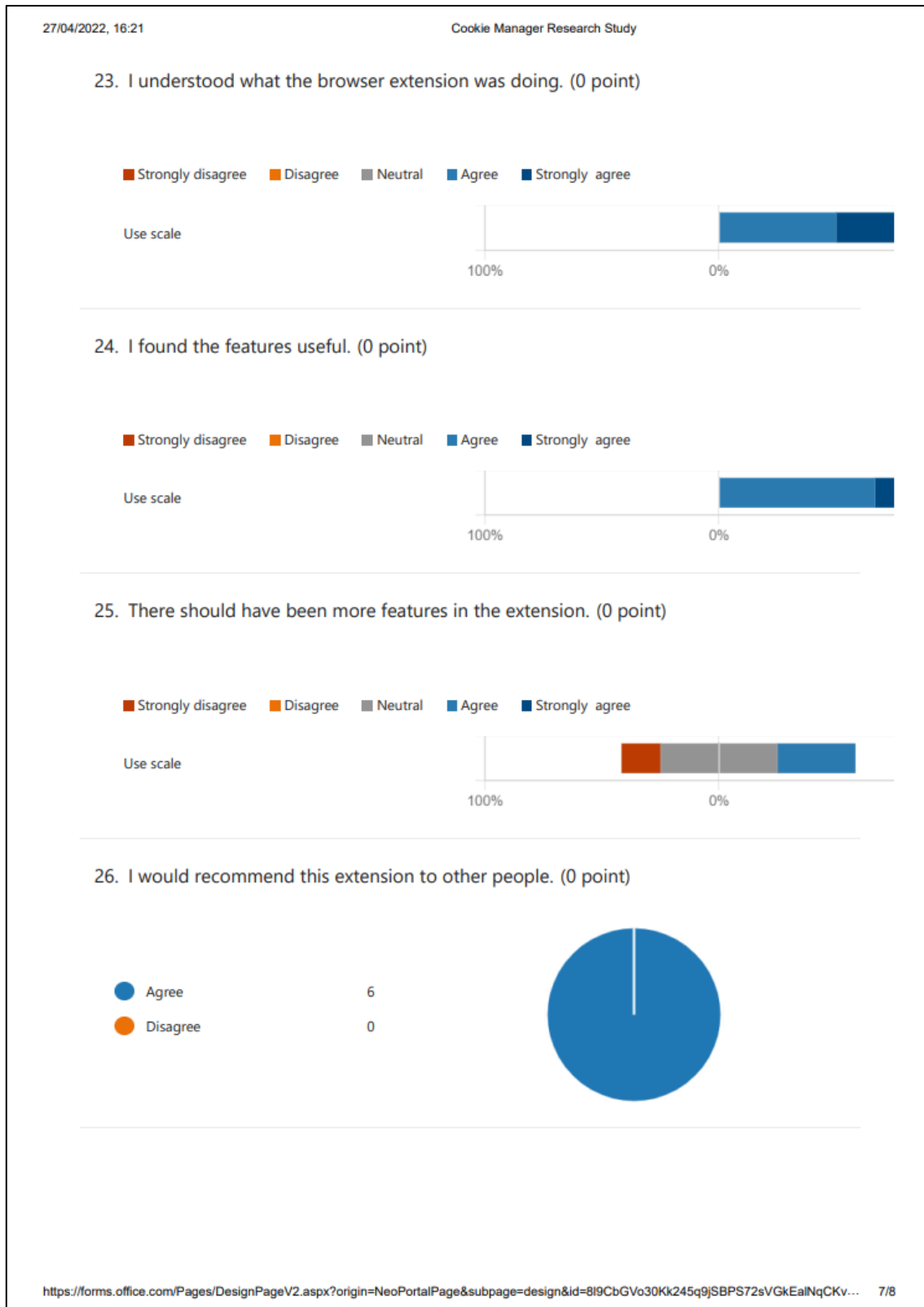**26. I would recommend this extension to other people. (0 point)**

● Agree   6
● Disagree   0

https://forms.office.com/Pages/DesignPageV2.aspx?origin=NeoPortalPage&subpage=design&id=8I9CbGVo30Kk245q9jSBPS72sVGkEalNqCKv···   7/8

27. Any other comments about the browser extension. (0 point)

Latest Responses

6
Responses

"Disabled buttons were confusing"

"Information on what 'blacklist' means would be useful as don't know what it is."

"Info section is useful to understand cookies."

Appendix C Raw Study Data

The raw study data has been submitted to the project system in a zip file.