A Usability Evaluation of Privacy Add-ons for Web Browsers

Matthew Corner[1], Huseyin Dogan[1], Alexios Mylonas[1] and Francis Djabri[2]

[1] Bournemouth University, Bournemouth, United Kingdom
{i7241812,hdogan,amylonas}@bournemouth.ac.uk

[2] Mozilla Corporation, San Francisco, United States of America
zerodegreedesign@me.com

Abstract. The web has improved our life and has provided us with more opportunities to access information and do business. Nonetheless, due to the prevalence of trackers on websites, web users might be subject to profiling while accessing the web, which impairs their online privacy. Privacy browser add-ons, such as DuckDuckGo Privacy Essentials, Ghostery and Privacy Badger, extend the privacy protection that the browsers offer by default, by identifying and blocking trackers. However, the work that focuses on the usability of the privacy add-ons, as well as the users' awareness, feelings, and thoughts towards them, is rather limited. In this work, we conducted usability evaluations by utilising System Usability Scale and Think-Aloud Protocol on three popular privacy add-ons, i.e., DuckDuckGo Privacy Essentials, Ghostery and Privacy Badger. Our work also provides insights into the users' awareness of online privacy and attitudes towards the abovementioned privacy add-ons; in particular trust, concern, and control. Our results suggest that the participants feel safer and trusting of their respective add-on. It also uncovers areas for add-on improvement, such as a more visible toolbar logo that offers visual feedback, easy access to thorough help resources, and detailed information on the trackers that have been found.

Keywords: Usability, Privacy, Browser Add-ons.

1 Introduction

Currently, the web is a life-changing service that users visit on a daily basis. The web affects every aspect of our life such as the way we do business, interact with others, entertain ourselves and access information. However, the web comes with a number of vectors that might compromise users' privacy. One of the prominent ways in which privacy is compromised is through tracking. Specifically, there is an incessant effort from most services on the web to track the behaviour of their users. These services collect data in order to find out as much as they can about their user base, including who they are in contact with, and their online purchases [1]. Moreover, trackers now-

adays use a number of client-side technologies for tracking users, other than cookies [2].

Tracking web users can take place for legitimate purposes (e.g. analytics, personalised user experience, etc.). However, extensive user tracking can lead to behavioural profiling, which provides unauthorised access to a user's personal data. The notion of constructing a 'profile' of a user through collected personal data is also highlighted in [3] and [4]. Roesner et al. [5] found more than 500 unique trackers in a corpus of 1000 websites (from very popular to lesser-used websites). Similarly, Schelter and Kunegis [6] found third-party trackers on more than 3.5 billion websites. This suggests that the sites users visit are most likely not the only entities tracking their behaviour. In the past, tracker blocking has not been offered as an out-of-the-box browser privacy mechanism [7]. However, currently two popular desktop browsers (i.e. Opera and Firefox) enable it by default. Firefox blocks by default if the user is browsing in a private window, but this is not default behaviour for the normal browser window. Furthermore, a variety of privacy add-ons are now available in the add-on repositories of web browsers, which offer protection against web tracking [8].

However, studies suggest there is room to improve the usability of privacy add-ons [9-11]. Schaub et al. [9] found in a privacy add-on study that whilst people tend to be aware of tracking, they do not know the specific details. This holds as the add-ons offered only a limited amount of information regarding who is running the trackers and for what means the data is collected. The use of an add-on increased the users' awareness of online tracking. Marella et al. [10] studied the effectiveness of privacy add-ons in communicating awareness of privacy risks. Their findings suggest users feel a sense of security just from installing the add-on, but generally they remained unsure as to why their data was being collected. A usability study by Leon et al. [11] found that participants had trouble configuring their privacy add-ons, and wrongly assumed they were blocking trackers due to not understanding the user interface or receiving much feedback from it.

Studies in this area show that concern towards online privacy is existent [12-14]. According to [12], nearly 90% of Internet users in Britain are concerned about their online privacy. McCoy et al. [13] found that the intrusiveness of online advertisements can reduce the users' desire to return to a website, due to increased irritation with advertisements. Additionally, according to [14], web users who consider online privacy protection measures are targeted by the NSA for surveillance.

In this context, this work uses a survey with 30 participants in order to evaluate the usability of three popular privacy add-ons with varying user interface styles, namely: DuckDuckGo Privacy Essentials, Ghostery and Privacy Badger. With regard to their Firefox user base, Privacy Badger has more than 500,000 users, DuckDuckGo Privacy Essentials has more than 700,000 users, and Ghostery has more than 1,000,000 [15].

The aim of the work is also to understand users' awareness along with their feelings of trust, concern, and control towards the add-ons. Participants interacted with one of the three add-ons through task-based scenarios whilst thinking aloud during a video screen capture. Further insight was gathered through three questionnaires, which the participants completed themselves at different points during the exercise.

The structure of the paper is as follows: Section 2 focuses on the user interface analysis of the privacy add-ons, Section 3 presents our methodology and Section 4 presents our findings. Finally, Section 5 concludes the paper and provides suggestions for future work.

2 User Interface Analysis of the Privacy Add-ons

This section compares interface elements for three popular privacy add-ons, namely: i) DuckDuckGo Privacy Essentials[1], ii) Ghostery[2], and iii) Privacy Badger[3]. Testing the effectiveness of the add-ons' tracker detection is not within scope for this study. Instead, its focus is on the usability of the add-ons and the feelings of the users towards them. In this regard, this section compares for each of the aforementioned add-ons: a) its toolbar icon, b) its main interface panel, and c) its help support (online webpages, help resources).

Fig. 1. Toolbar Icons for DuckDuckGo Privacy Essentials (Logo & Grade), Ghostery and Privacy Badger

Fig. 1, shows the toolbar icons for the three add-ons that are in scope of this work. The toolbar icon for DuckDuckGo Privacy Essentials displays either the DuckDuckGo logo or a letter to represent the visited website's privacy grade, which will be covered later in this section. If the add-on is calculating the grade, or the user has the browser settings or a new tab open, the logo will be displayed in the toolbar icon. The toolbar icon for Ghostery displays only the number of trackers detected on the website the user is currently visiting. Similarly, Privacy Badger shows the number of trackers blocked. The count on the Privacy Badger icon will turn amber when it goes above zero.

Figures 2 and 3 show the main interface panel of each add-on, which appears when the user clicks the toolbar icon. DuckDuckGo Privacy Essentials has a search bar at the top for the user to use the DuckDuckGo search engine. The privacy grade below is calculated based on: a) a rating of the site's privacy practices, b) the presence of trackers, and c) whether an encrypted connection is available. Data for the aforementioned appear below the grade and clicking on their widgets will reveal a more detailed screen (see Fig. 2a).

---

1 https://duckduckgo.com/app
2 https://www.ghostery.com/
3 https://www.eff.org/privacybadger

In the green area below 'Privacy Practices', the user can disable privacy protection for that website, which will add it to the whitelist. Moreover, the 'Manage Whitelist' link allows the user to add sites to the whitelist, and 'Report Broken Site' lets the user contact the developer if the add-on has impaired the functionality of the website. At the bottom of the home screen the 'top offender' trackers are displayed, i.e. the ones the user has encountered most across the websites they have visited. 'All Tracker Networks' takes the user to a new screen listing all the trackers the add-on has encountered.

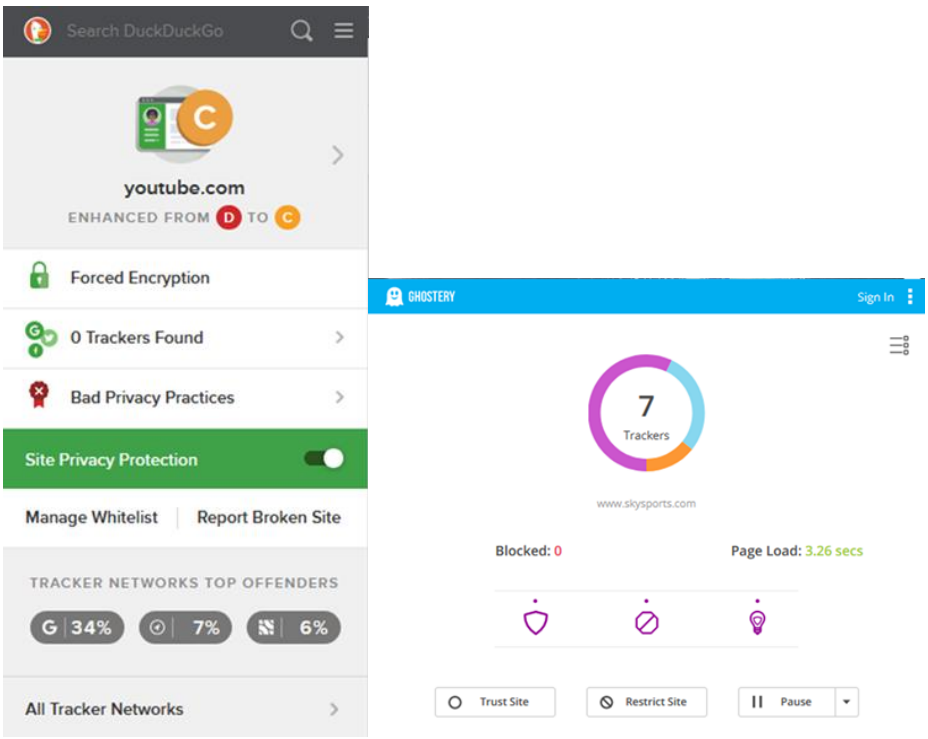

Fig. 2. Main Panel for: a) DuckDuckGo Privacy Essentials, and b) Ghostery (Simple View)

Fig. 2b, shows Ghostery's main panel in simple view, which displays the number of trackers found, the number of trackers blocked and the time that the visited site took to load. More advanced features can be interacted with via the purple symbols, as can the buttons to trust or restrict a site and pause the add-on. A more detailed view can be accessed by clicking on the list symbol in the top-right of the simple view, shown in Fig. 2b, which has a compressed version of the simple view to the left and a list of the found trackers to the right. The trackers are categorised based on their purpose; for example, Analytics, Essential or Advertising. More information for each tracker can be displayed by clicking on them, with the option to follow a hyperlink to a full tracker profile. Trackers can also be trusted or blocked on an individual basis.

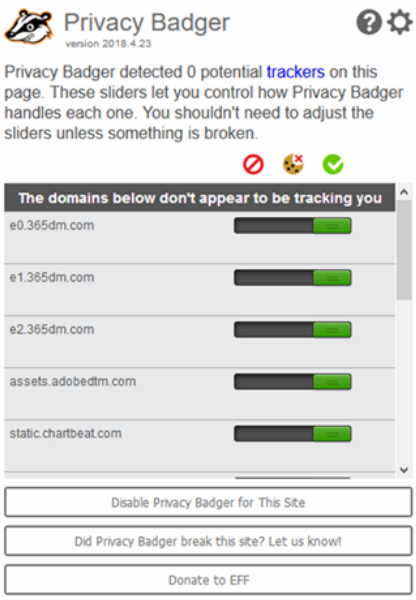

Fig. 3. Main Panel for Privacy Badger

At the top of the Privacy Badger interface the user has buttons for help or to access the settings (see Fig. 3). The add-on shows how many potential trackers are on the current page, it will block a tracking domain if it is encountered on three or more visited websites. The list in the centre of the interface displays all the found trackers. The slider bars allow the user to block entirely, block the cookies for, or trust that particular tracking domain. At the bottom of the interface, a button can be used to turn off the add-on for that site, which adds it to a whitelist. Users can report if the add-on has broken website functionality or click a button to donate money to the developers.

All three privacy add-ons have an introductory webpage that opens in the browser once the add-on is installed, with varying levels of detail. Further help can also be accessed within the add-ons themselves. Ghostery has the options of either a one-click or custom setup during installation.

In DuckDuckGo Privacy Essentials, the introductory webpage can be reopened by clicking on 'Learn More' within the add-on's settings menu. From this webpage, it is possible to navigate to a help library. Ghostery has a help button within its options menu, where the user can access frequently asked questions (FAQs) and support. Privacy Badger's help button, in the top-right of the main interface, reopens the add-on's introductory webpage. By clicking on the hyperlinked 'trackers' text an FAQs page can be accessed.

Finally, Table 1 summarises the comparison of the graphical interface features available across the add-ons used in this study.

Table 1. Comparison of Add-on Features

Add-On Feature	DDG Privacy Essentials	Ghostery	Privacy Badger
Enable / Disable for this Site	✓	✓	✓
Report Broken Site	✓	✓	✓
Count of Detected Trackers	✓	✓	✓
List of Found Trackers	✓	✓	✓
Allow/ Block Individual Tracker Domains	✗	✓	✓
Specifically Block Cookies for a Domain	✗	✗	✓
Access to FAQs / Help Pages	✓	✓	✓
Domain Whitelist	✓	✓	✓
Donate to Developer	✗	✗	✓
Add-on Settings Menu	✓	✓	✓
Choice of Simple or Detailed Interface	✗	✓	✗
Page Load Time	✗	✓	✗
Sign in with Account	✗	✓	✗
Pause Add-on Protection	✗	✓	✗
Submit a New Tracker	✗	✓	✗
Default or Custom Installation Setup	✗	✓	✗
Choice of Advanced Features	✗	✓	✗
Search Engine Bar	✓	✗	✗
Force Encrypted Connection	✓ (if available)	✗	✗
Website Privacy Practices	✓	✗	✗
Website Privacy Grade	✓	✗	✗

3 Methodology

A survey was carried out to evaluate the usability of the privacy add-ons through a comparative analysis, as well as to understand users' awareness of online privacy and attitudes towards the add-ons. The attitudes focused on were those of trust, concern, and control. The participants were introduced to three scenarios related to their designated add-on, whilst thinking aloud, and the completion of three questionnaires. Think aloud encourages participants to vocally share their thoughts and feelings whilst interacting with the user interface of a product [16]. We carried out a pilot run-through before commencing the study with the participants, to allow any potential issues to be found and corrected [17].

For the survey, 30 participants were recruited in total and were assigned one of the add-ons via round-robin. However, the very first allocation was randomised. The participants were evenly allocated with 10 individuals per add-on, they were given a £10 Amazon voucher as an incentive to participate. Participants were not computer science students, nor did they have an educational background in this field. They were older than 18 and there was no bias towards age, gender, educational background, web browser preference, or current level of online privacy awareness when recruiting.

Most participants fell into the 18-24 age bracket, with 19 (63%) participants being in this age range. 9 (30%) were in the 45-54 group and the remaining 2 (7%) fell into the 55-64 age bracket. The majority of participants were male, forming 57% of the participant group, which consisted of 17 males and 13 females. 11 participants (37%) held a bachelor's degree, whilst another 11 (37%) held GCSEs (General Certificate of Secondary Education) or equivalent. 7 individuals (23%) possessed A-Levels or equivalent and 1 participant held a master's degree. A-levels are the traditional qualifications that are offered by schools and colleges for students aged between 16 and 19 in the UK. Most participants were Google Chrome users, with 21 of 30 participants (70%) preferring this browser. 4 participants (13%) preferred Safari. Mozilla Firefox was the choice of 3 participants (10%) and 2 of the 30 (7%) chose Internet Explorer as their preferred browser.

The tasks were completed using Mozilla Firefox or Google Chrome within an Ubuntu Linux Virtual Machine. A video screen capture and an audio recording of task completion were taken, due to the use of think-aloud. Recordings were deleted once they had been analysed and transcribed. Within the browser, either the DuckDuckGo Privacy Essentials, Ghostery or Privacy Badger add-on was used. The add-on was uninstalled once each participant had completed their tasks and questionnaires.

Participants were given information sheets and consent forms prior to the testing commencing. They were also given an instruction sheet. The three questionnaires were constructed in Google Forms. A Pre-Task questionnaire was used to gather demographic information and the level of agreement with privacy-related statements. A System Usability Scale (SUS) questionnaire was given to the participants upon completion of the tasks. A final Post-Tasks questionnaire was also given to gather responses to measure perceived concern, trust, and control when using the selected privacy add-on. Participants could share any other thoughts, feelings, or suggestions they had.

3.1 Pre-Tasks Questionnaire

Prior to installing the add-on, this initial questionnaire asked participants for some basic demographic information: age, gender, highest completed level of education and preferred web browser. They were also asked how strongly they agreed or disagreed with three statements using a 5-point Likert scale, which were used to classify their attitude towards privacy with Westin's Privacy Index [18]. To get an idea of awareness, participants were asked to define 'web cookie', 'tracker' and 'browser add-on'.

3.2 Scenarios and Tasks

After completing the first questionnaire and asking any questions, the video screen capture and audio recording started. The participants' first task was to install the assigned add-on and quickly familiarise themselves with it - the add-on store page was open for them in the web browser. All participants were instructed to read the introductory webpage, which opens in the browser once installation is complete.

Then, participants completed tasks that were split into three scenarios focusing on i) government surveillance, ii) price discrimination, and iii) social stigma. More specifically, the three scenarios were: i) 'Imagine that you want to update yourself with recent news on "Brexit". Using the Buzzfeed website, browse and examine pro-Brexit articles', ii) 'Imagine that you want to book a two-week holiday to a destination of your choice in September of this year. Using the TravelSupermarket website, browse the possibilities they have on offer', and iii) 'Using the Boots website, search for sexual health and browse the products and advice available'. Tasks incorporated interactions with features common across the add-ons. Participants spent 1-2 minutes browsing as per the scenario, then completed the specific tasks given to them.

For the first scenario, participants had to whitelist the Buzzfeed[4] website, meaning the trackers present on the site will not be blocked. Then, DuckDuckGo Privacy Essentials and Privacy Badger users had to navigate to the help page, whilst Ghostery users had to find the FAQs.

In the second scenario, the participants were asked to find how many trackers were blocked on the TravelSupermarket[5] website by their assigned add-on. They also had to look for a list to investigate what trackers were found, and what information the add-on gives about them.

Prior to commencing the third scenario, DuckDuckGo Privacy Essentials and Privacy Badger users had to disable their add-on, Ghostery users had to pause it for 30 minutes. Participants then had to find the number of trackers present on the Boots[6] website before searching for sexual health as part of the scenario. The video screen

[4] Buzzfeed is an internet media and news website: https://www.buzzfeed.com/

[5] TravelSupermarket is a website for comparing travel deals: https://www.travelsupermarket.com/

[6] Boots is a health, beauty and pharmacy retailer that is popular in the UK: https://www.boots.com/

capture and audio recording was stopped and saved once the third scenario had been completed.

After completing the three scenarios, participants completed a System Usability Scale questionnaire for their assigned add-on via a Google Forms link [19]. At the end of the form, participants were asked to share any further thoughts, comments, or suggestions they had regarding the add-on's usability. An examination of 500 studies into SUS found the average score to be 68 out of 100 [20].

3.3 Post-Tasks Questionnaire

The final questionnaire gathered responses to collate participants' feelings of trust, awareness, concern, and control towards their online privacy when using their assigned add-on. Participants were also asked to elaborate on what they think makes the add-on trustworthy or untrustworthy. They were asked how strongly they agree or disagree with the below statements, using a 5-point Likert scale:

1. 'I would feel safer browsing the Internet when using a privacy add-on'
2. 'I would trust the legitimacy of a website more if the privacy add-on reflected it'
3. 'The privacy add-on informed me about the purpose of the trackers it identified'
4. 'I would be reluctant to use a website if it asked me to disable my privacy add-on'
5. 'Overall, the add-on is trustworthy'

Participants were then asked to explain what makes the add-on trustworthy, or untrustworthy.

4 Findings

4.1 Westin's Privacy Index

Most participants fell into the Pragmatist category, 23 of the 30 (77%) had this initial attitude towards privacy. 5 participants (16%) were categorised as Unconcerned and the remaining 2 (7%) were Fundamentalists [18].

4.2 Awareness of Related Terms

When asked to define a 'web cookie', overall the participants appeared to understand the notion. Whilst not all offering full definitions, most participants defined part of what cookies can do and seemed to have a general understanding. Potentially due to the connotations of the word 'tracker' itself, participants were generally aware of the fact that a tracker watches, or monitors, online behaviour. First-party and third-party trackers were mentioned in the responses from the participants. 18 out of the 30 users appeared to have awareness of browser add-ons. Out of these 18 participants, 4 made specific mention of encountering them in the form of an ad-blocker or a VPN. It was generally understood that an add-on is a supplemental software installation for a web browser, to perform a desired set of functions.

4.3 System Usability Scale Scores and User Comments on Usability

System Usability Scales Scores. Ghostery received the highest usability score from participants, with an average of 79. DuckDuckGo Privacy Essentials and Privacy Badger both scored below average, with scores of 60 and 62 respectively. Participants were also asked to give qualitative comments on the usability of the add-on they interacted with.

Out of the 10 DuckDuckGo Privacy Essentials users we found that: 6 somewhat or strongly agreed that they would like to use the add-on frequently, whilst 2 somewhat or strongly disagreed. Just under half (i.e. 4) found the add-on to be unnecessarily complex and another 4 disagreed with this statement, the remaining 2 stayed neutral. 3 participants agreed that the add-on was easy to use, however the majority (i.e. 8) disagreed that there was too much inconsistency in the add-on. Moreover, when asked whether they needed to learn a lot of things before they could get going with the add-on, 6 participants disagreed with the statement whilst 4 somewhat or strongly agreed that they did. Finally, 4 out of 10 participants agreed that they felt very confident using the add-on.

Out of the 10 Privacy Badger users: 7 agreed that they would like to use the add-on frequently, with the other 3 disagreeing. No participants agreed that they found the add-on unnecessarily complex; 6 somewhat or strongly disagreed and 4 were neutral to this statement. Less than half (i.e. 4) agreed that they thought the add-on was easy to use, 3 somewhat or strongly disagreed and 3 did not agree nor disagree. The majority (i.e. 7) agreed that they would imagine most people learning to use the add-on quickly. Just over half (i.e. 6 users) agreed that they felt very confident using the add-on, with 2 disagreeing and 2 answering neutrally. Finally, 4 out of 10 participants agreed that they needed to learn a lot of things before they could get going with Privacy Badger, 5 disagreed with this statement.

Regarding the 10 Ghostery users, our results suggest that: the majority (i.e. 7 users) agreed that they would like to use the add-on frequently. Nearly all (i.e. 9 users) disagreed that they found the add-on unnecessarily complex, the same number of participants agreed that they thought the add-on was easy to use. All 10 participants disagreed that they would need the support of a technical person to be able to use the add-on and disagreed that they found the add-on cumbersome to use. 9 participants agreed that most people would learn to use the add-on quickly, but just over half (i.e. 6 participants) somewhat or strongly agreed they felt very confident using the add-on. Finally, most (i.e. 8 users) disagreed that they needed to learn a lot of things before they could get going with Ghostery.

System Usability Scale Comments. Participants were able to offer comments or suggestions for usability improvements as part of the SUS questionnaire.

For DuckDuckGo Privacy Essentials, P12 said ‘When looking for a help page, I'd want to be taken to a different page from the introduction, one with more information.’ P30 commented ‘the help section was not obvious’ and P21 thought ‘it was not easy to find the help page’. P27 answered that ‘help and explanations need to be clearer’. These thoughts were echoed by comments made during the think-aloud exer-

cise. P1, who used Ghostery during this study commented that 'the only difficulty was finding the FAQs page' but felt that navigating to it made more sense in hindsight. P10 also used Ghostery and thought the 'FAQs was harder to find, but hardly necessary as the add-on was so easy to use'. One of the Privacy Badger users, P8, commented that they 'would have preferred the help link to go to an FAQs website, then have some step by step guides'.

P15 felt the toolbar icon for DuckDuckGo Privacy Essentials needed to be more visible. Also, P18 commented in their SUS questionnaire that the icon is also grey, and they felt it gave no visual feedback, expecting help when hovering the mouse over elements of the user interface. P26, who interacted with Privacy Badger, suggested 'visual aids that could make the usability easier for people who are not tech-minded'.

P10 commented that in Ghostery it was 'simple to see the results'. In terms of the interface layout, P19 thought the button to swap from the simple view to the detailed view 'was a little too close the drop-down setting menu and was a little confusing'. P25 similarly commented that 'the menu bar needs to be more clear'. P10 did appreciate the breakdown of the found trackers and P13's awareness was increased by using Ghostery, they were 'impressed with how many trackers there are when you use the web'. P14 also commented on the information for trackers that Privacy Badger found, they thought the add-on 'could have been a little clearer when breaking down the tracking service'.

4.4 Perceptions of the Privacy Add-ons

Fig. 4, presents the results from the post-tasks questionnaire. All three add-ons averaged a score of 4.5 when participants were asked if they would be reluctant to disable the add-on at a website's request, signifying that a site would be deemed unsafe and untrustworthy if it made any attempt or request to turn off the add-on. Participants deemed Privacy Badger to be the least informative regarding the purpose of the trackers it found, receiving an average score of 2.1. DuckDuckGo scored 2.8 and Ghostery was considered the most informative with 3.8.

When participants were asked if they would trust the legitimacy of a website more if the privacy add-on reflected it, DuckDuckGo received an average of 4.3. Ghostery and Privacy Badger averaged at 3.7 and 4 respectively. DuckDuckGo received the highest average of 4.2 when participants had to express if they feel safer browsing the internet with the privacy add-on. Ghostery and Privacy Badger both averaged at 4.

Participants were also asked what made the add-on they interacted with trustworthy, or untrustworthy. For DuckDuckGo Privacy Essentials, P3 'didn't feel especially trusting of it' due to a lack of awareness of the add-on itself, mentioning it may even be a 'ploy to access my data'. On the other hand, P12 said 'the add-on explains its purpose simply, it seems good for a novice to get to grips with'. P6 was unsure of the add-on's trustworthiness as there was not enough to 'give the user any useful information'. P19 was also unsure as they felt there was 'no visual feedback…or severity of the tracker being blocked'. P9 and P30 both felt the add-on was trustworthy; P9 felt

it ‘goes into frank detail about the potential privacy breaches’ and P30 said the add-on is ‘very to-the-point’.

A number of participants who interacted with Ghostery felt trusting due to the information given to them by the add-on. P22 said ‘it told me which trackers there were and how many’. P10 felt it ‘clearly shows what it does’ and is ‘well-presented and written’. P25 thought the add-on was reliable as it ‘gives you a lot of information on the trackers’, and P28 trusted Ghostery as ‘it helps the user identify unwanted trackers and block them straight away’. However, P16 was neither trusting nor distrusting of Ghostery as they ‘don’t fully know whether they have listed all the possible trackers’. P7 did not trust Ghostery due to the ‘product introduction, marketing, and image’.

P8, who used Privacy Badger, trusted the add-on as it ‘helps to identify numerous trackers’. They also commented ‘it would help to have more information on why they were blocked though’. P17 found the add-on trustworthy because they felt ‘it gave a list of most, if not all, trackers’. P23 and P26 neither trusted nor distrusted Privacy Badger. P23 said ‘it shows the trackers but does not give enough information about the trackers’. P26 thought there was ‘not enough explanation of the trackers it was identifying and disabling’.

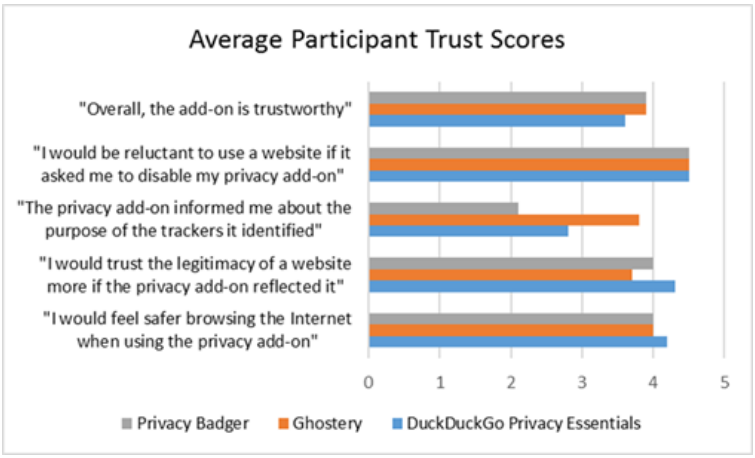

Fig. 4. Average Participant Trust Scores. Scores of 1 indicate strongly disagree, whilst scores of 5 are for strongly agree.

4.5 Think-Aloud Findings

Accessible for less IT-savvy users. After installing their assigned add-on, participants read the introductory webpage which opens once installation is completed. P9 and P12, who both used DuckDuckGo Privacy Essentials, felt the introductory page was sufficient and simple; P12 said ‘it is pretty straightforward to follow’. P21 was unsure whether the add-on was fully installed at this stage, but commented the introduction was ‘explaining things at a human level’ which they found helpful as they described themselves as ‘not IT-literate’. P27 believed some definitions of related

terms would be beneficial for inexperienced users and P30 praised the images on the page for 'showing exactly where certain aspects are', in terms of the user interface.

P25, who interacted with Ghostery, also commented that some definitions of terms on the introduction page would be beneficial. P16 felt step-by-step instructions for using the add-on would help, as they thought the page had enough information but lots to read. P7 said the introduction was 'way too full of jargon for your normal person'. P13 praised the use of images to show the layout of the add-on's user interface.

On Privacy Badger's introduction page, P8 said the prompt to 'take the tour' should 'almost slide across like a PowerPoint instead of coming down to read'. They felt the introduction improved their awareness of trackers, commenting 'there is the advertising stuff, and then a lot more deeper that I wasn't aware of before'. P14 was content with the information, saying 'it has broken everything down for you'. P20 commented 'I like the little pictures… I like visual things', praising the use of images to introduce the user. However, P26 felt the page 'doesn't really tell you a lot about what is going on' and would want to see a breakdown of what exactly the add-on does.

When attempting to whitelist the site using DuckDuckGo Privacy Essentials (i.e. during the first scenario), P6 commented 'it is not obvious to me how I would add that as a novice… you'd just want to press a button that is immediately visible to you'. This can be achieved with the 'Site Privacy Protection' toggle on the main interface, possibly suggesting a lack of awareness of related terms, which has also been highlighted by other participants. When P12 saw the green 'Site Privacy Protection' toggle, they comment that 'it is already set' as trusted, when this actually meant the add-on was enabled for that particular site. A site can also be trusted by adding it to the whitelist. P21 was familiar with the concept of a whitelist and commented 'that is a clunky way of having to add it' once they had completed the task.

Keep the Options Tab Open. When navigating to DuckDuckGo Privacy Essentials' whitelist, it opens in a new browser tab. A few participants commented on this tab closing itself as they navigated between it, the Buzzfeed website, and the add-on. P3 went to copy the Buzzfeed URL into the whitelist and exclaimed 'oh it has gone' as they navigated to a different tab. When the tab closed for P12, they said 'that is annoying, you lose everything if you click off'. P18 commented 'oh it went away… I would have expected it to stay open, so I can copy and paste'.

Visible Toolbar Icon with Visual Feedback. A number of users commented on DuckDuckGo Privacy Essentials' toolbar icon. P9 was looking for a duck logo to access the add-on and felt the icon displaying the privacy grade did not stand out. P18 said 'doesn't look like it is active… I would expect something other than mono'; P27 commented 'Is it on? It is not coloured'. During the second scenario, P3 commented on receiving no prompts from the add-on whilst browsing. They said 'because it has not said anything to me, I don't know what it is up to… I've just the assumption it is making what I'm doing safer'.

When P10 whitelisted the Buzzfeed website using Ghostery, they commented ‘well that was super easy’. P1 saw the add-ons toolbar icon go grey and said, ‘I assume that is trusted’, they rechecked the add-on and confirmed with ‘yeah, it is trusted’.

During the first scenario, P2 commented on Privacy Badger’s toolbar icon. They said ‘I’ve noticed there is a green box with a zero…not quite sure what that means’. Upon seeing how many trackers the add-on had identified, they exclaimed ‘wow, 46 potential trackers on this page…that is a lot’. P5 also commented on the toolbar icon, saying ‘so there is none there… that is what the little zero is telling me… there is nobody tracking me’. However, this number in the toolbar icon represents the number of trackers blocked, rather than the number found.

Obvious Access to Thorough Help Resources. There were comments related to a perceived lack of visible help for the DuckDuckGo Privacy Essentials add-on. P6 commented they were looking for a help page ‘which is not very helpful because it is not there straight away…unless I am being stupid’. Upon being navigated back to the introduction page whilst searching for help, P12 asked ‘Nope, why has it sent me there? I would expect something more detailed’. P21 believed ‘there is not an obvious place to go for help’. P27 said that ‘the whole point of help, you shouldn’t have to look for help’.

P4 felt the FAQs page for Ghostery was quite hidden and thought the buttons for the detailed view and options menu were too similar visually. P19 had the same opinion on this. P28 commented ‘that is really hidden away’ with regard to the FAQs page.

When P26 was navigated back to Privacy Badger’s introduction page after clicking the help button they said, ‘I guess it does sort of help you…but it is not very clear’. P17 did not like the fact they were sent back to the introduction page and wanted to see definitions for what specific terms meant. P11 thought they had made a mistake at this point, they thought ‘for help it feels like it needs a little more information, or something different to what I’ve already learnt from using it’.

Detailed Tracker Information. When scrolling through the list of trackers found by the DuckDuckGo Privacy Essentials add-on, P3 saw some they did not recognise the names of and said, ‘it would be nice if there was more to say what they are, and what they are up to’. P6 wanted more information, commenting ‘it is not telling me what those trackers would be tracking’. P21 did not understand why a tracker would be identified but not described, P24 said ‘it does not feel entirely adequate’.

Whilst they were examining the list of trackers found by Ghostery, P10 said ‘I like this breakdown’ and praised the amount of detail when navigating to the full tracker profile. P22 said ‘for me, it is enough’ and P25 commented ‘oh, it gives you a little description. That is good’.

Whilst they scrolled through the list of found trackers in Privacy Badger, P8 said ‘Some of them I recognise, some of them I don’t…it would be nice to know where they are coming from and what they are doing’. P11 thought it would be interesting to hover over the name of the tracker to get more information on it, P26 also wanted

more information on them. P23 commented ‘I don’t know what these trackers are, it is just a name, that is it’. Similarly, P17 said it ‘tells you the name, not what it is’.

Clear Differentiation Between Blocked and Found. For the second scenario, participants had to identify the number of trackers blocked by the add-on and find a list showing what trackers were found. All participants using DuckDuckGo Privacy Essentials correctly identified the number of blocked trackers from information shown on the main user interface. P6, P9 and P30 commented on finding that task easy.

When examining the Ghostery add-on to identify the number of trackers that had been blocked, 4 out of the 10 participants thought the count of found trackers was the number that had been blocked. The rest of the participants identified the number of trackers that Ghostery had blocked. P22 and P25 both commented that they would have expected more trackers to be blocked out of what had been found. P4 commented on the toolbar icon causing confusion during this task, as ‘the 13 up there was quite distracting, but it is actually 0 blocked’. P1 incorrectly said ‘I assume its four’ when looking at the toolbar icon to identify the number of trackers blocked.

Out of the 10 participants interacting with Privacy Badger, half correctly identified the number of trackers blocked. P26 was expecting a more obvious confirmation of how many trackers had been blocked. P29 referred to the toolbar icon saying, ‘don’t like it says zero up there, I wouldn’t know unless I purposely clicked on it’.

Invasiveness of Tracking. The third scenario asked participants to pause or disable their relative add-on prior to browsing for sexual health on the Boot’s website. At the end of the browsing time, they had to identify the number of trackers present on the site.

As P9 disabled DuckDuckGo Privacy Essentials they said, ‘Oh that is a lot of trackers’. P21 commented ‘I am not clicking on Viagra, I will have all sorts of stuff on my IP address’. P9 noticed the tracker count increasing, ‘I would be more cautious… I’d definitely think about getting something like this that protects you’. P12 said that whilst ‘searching sensitive, private details, I would not want adverts appearing on my social media’. P15 commented ‘it is really concerning...that is just unbelievable, you don’t know what is going on in the background’, and P18 referred to it as ‘quite scary’. Most participants seemed to feel quite strongly about privacy during this part of the task, with some commenting that the exercise had increased their awareness.

Out of the 10 participants who used Ghostery, 7 paused for 30 minutes whilst the other 3 just clicked the pause button without modifying the time. When identifying the number of trackers present, P13 said ‘I like the fact I now know…I can block trackers’. P22 commented ‘it has opened my eyes a bit… I am more concerned now than I was before doing this’. P28 initially said the tracker amount doesn’t bother them too much as ‘I don’t really care what people think’ before stating ‘actually no, I wouldn’t want that coming up on my Facebook’. Likewise, P19 said ‘you don’t really want those ads appearing’.

During this exercise, P5 said ‘what I am finding more disturbing…I wasn’t aware how many people could potentially be tracking you… that has been quite an eye opener for me’. After P5 had disabled Privacy Badger, they commented ‘the more personal something becomes, I’m thinking oh gosh how many people are going to be out there tracking me’. During the exercise they shared thoughts on their experience with targeted ads, ‘The one thing I find so frustrating…it drives me absolutely nuts’. Comments were also made on the ethics of the trackers. P8 thought ‘there is a lot of stigma around people collecting information they shouldn’t be’. P11, another Privacy Badger participant, said ‘I’m fairly against all this information being tracked and stored…if people are doing it, I like to know they’re doing it and why’. P17 commented ‘considering I haven’t made an account, I haven’t given them permission’.

5 Conclusions

With the proliferation of web tracking the importance of privacy preserving add-ons, which extend the out-of-the-box protection offered by web browsers, increases. However, whilst preserving and increasing the efficacy of blocking trackers is of paramount importance, so is the usability of the add-ons and user awareness. In this regard, this work mounted a survey which aimed to gain thoughts and feelings towards three popular anti-tracking add-ons (i.e. DuckDuckGo Privacy Essentials, Ghostery and Privacy Badger) from participants, and to measure their usability. The websites and tasks chosen sought to encourage interaction with the common features of the add-ons whilst using predominately realistic scenarios.

Based on participant responses, the level of information given by the add-on, including on the trackers it has found, may influence their level of trust towards it. There were also comments from participants on the inclusion of definitions or terminology to improve their understanding. A possible improvement could come from their wish of having a help button always visible on the main interface, or it being one of the first options visible when clicking to open the options menu. A glossary of related terms could potentially be included here. Ensuring this button is distinguishable from others would reduce potential confusion of functions. Rather than the help link going back to the introduction page, it should navigate to an FAQs page or some sort of knowledge bank. Users felt that being navigated back to an introductory web page was not helpful. Help resource suggestions from users included a glossary of online privacy related terms, a search function for questions, and step-by-step guides.

Additionally, information on the trackers should be given. Participants were curious as to the purpose and origin of the trackers they found. Not knowing the identity of certain trackers caused concern.

It may be beneficial for the toolbar logo to contain colour and be immediately visible, for the user to know the add-on is functioning by offering visual feedback.

For future work we plan to investigate: a) producing a prototype for a more usable privacy add-on, b) the proposition of an initial set of usability heuristics for online privacy add-ons, and c) the proposition of a perceived user threat model and potential ways of countering them.

References

1. Bujlow, T., Carela-Español, V., Solé-Pareta, J., Barlet-Ros, P.: A survey on web tracking: mechanisms, implications, and defenses. Proceedings of the IEEE 105(8), 1476-1510 (2017).
2. Belloro, S., Mylonas, A.: I know what you did last summer: New persistent tracking mechanisms in the wild. IEEE Access 6, 52779-52792 (2018).
3. Liu, D., Gao, X., Wang, H.: Location privacy breach: Apps are watching you in the background. IEEE 37th International Conference on Distributed Computing Systems, 2423-2429 (2017).
4. Sipior, J. C., Ward, B. T., Volonino, L.: Privacy concerns associated with smartphone use. Journal of Internet Commerce 13(3-4), 177-193 (2014).
5. Roesner, F., Kohno, T., Wetherall, D.: Detecting and defending against third-party tracking on the web. In: Proceedings of the 9th USENIX Conference on Networked Systems Design Implementation, pp. 1-12. USENIX, San Jose (2012).
6. Schelter, S., Kunegis, J.: Tracking the trackers: A large-scale analysis of embedded web trackers. Proceedings of the Tenth International AAAI Conference on Web and Social Media, 679-682 (2016).
7. Mylonas, A., Tsalis, N., Gritzalis, D.: Evaluating the manageability of web browsers controls. In: Accorsi, R., Ranise, S. (eds.) STM 2013, LNCS, vol. 8203, pp. 82–98. Springer, Heidelberg (2013).
8. Tsalis, N., Mylonas, A., Gritzalis, D.: An intensive analysis of security and privacy browser add-ons. In: Lambrinoudakis C., Gabillon A. (eds.) CRiSIS 2015, LNCS, vol. 9572, pp. 258-273. Springer, Cham (2015).
9. Schaub, F., Marella, A., Kalvani, P., Ur, B., Pan, C., Forney, E., Cranor, L. F.: Watching them watching me: Browser extensions impact on user privacy awareness and concern. In: NDSS Workshop on Usable Security (2016).
10. Marella, A., Pan, C., Hu, Z., Schaub, F., Ur, B., Cranor, L. F.: Assessing privacy awareness from browser plugins. In: Poster at the Symposium on Usable Privacy and Security (SOUPS) (2014).
11. Leon, P. G., Ur, B., Balebako, R., Cranor, L. F., Shay, R., Wang, Y.: Why johnny can't opt out: A usability evaluation of tools to limit online behavioural advertising. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 589–98. ACM, New York (2012).
12. Moth, D.: Econsultancy, https://econsultancy.com/89-of-british-internet-users-are-worried-about-online-privacy-report/, last accessed 2018/12/10.
13. McCoy, S., Everard, A., Polak, P., Galletta, D.: An experimental study of antecedents and consequences of online ad intrusiveness. International Journal of Human-Computer Interaction 24(7), 672-699 (2008).
14. Vincent, J.: Independent, https://www.independent.co.uk/life-style/gadgets-and-tech/news/nsa-reportedly-tracking-any-internet-users-who-research-privacy-software-online-9585250.html, last accessed 2018/12/10.
15. Mozilla Firefox Privacy & Security Add-ons, https://addons.mozilla.org/en-GB/firefox/search/?category=privacy-security&sort=users&type=extension, last accessed 2019/02/19
16. Nielsen, J.: Nielsen Norman Group, https://www.nngroup.com/articles/thinking-aloud-the-1-usability-tool/, last accessed 2018/12/10.
17. Preece, J., Rogers, Y., Sharp, H.: Interaction design: Beyond human-computer interaction. 4th edn. Wiley, Chichester (2015).

18. Kumaraguru, P., Cranor, L. F.: Privacy indexes: A survey of westin's studies. Institute for Software Research International, Carnegie Mellon University, Pittsburgh (2005).
19. Brooke, J.: SUS- A quick and dirty usability scale. Usability Evaluation in Industry 189(194), 4-7 (1996).
20. Sauro, J.: Measuring U, https://measuringu.com/sus/, last accessed 2018/12/10.