Characterizing the Use of Browser-Based Blocking Extensions To Prevent Online Tracking

Arunesh Mathur
Princeton University
Princeton, NJ
amathur@cs.princeton.edu

Jessica Vitak
University of Maryland
College Park, MD
jvitak@umd.edu

Arvind Narayanan
Princeton University
Princeton, NJ
arvindn@cs.princeton.edu

Marshini Chetty
Princeton University
Princeton, NJ
marshini@princeton.edu

ABSTRACT

Browser-based blocking extensions such as Ad blockers and Tracker blockers have provisions that allow users to counter online tracking. While prior research has shown that these extensions suffer from several usability issues, we know little about real world blocking extension use, why users choose to adopt these extensions, and how effectively these extensions protect users against online tracking. To study these questions, we conducted two online surveys examining both users and non-users of blocking extensions. We have three main findings. First, we show both users and non-users of these extensions only possess a basic understanding of online tracking, and that participants' mental models only weakly relate with their behavior to adopt these extensions. Second, we find that that each type of blocking extension has a specific primary use associated with it. Finally, we find that users report that extensions only rarely break websites. However when websites break, users only disable their extensions if they trust and are familiar with the website. Based on our findings, we make recommendations for designing better protections against online tracking and outline directions for future work.

1. INTRODUCTION

Online tracking presents numerous privacy risks to users. Third-party trackers present on multiple websites [13] collect sensitive information such as users' personal information, activities, and interests [26] without necessarily alerting users to this type of tracking. Many such third-parties also transmit the information they collect over insecure channels, impeding HTTPS adoption [13, 29]. Given the fact that tracking is on the rise and is often undesirable, users have been advised by numerous agencies, including the Federal Trade Commission (FTC) [14, 9], to take adequate steps to shield their information from such online tracking.

Users can protect themselves from online tracking by deploying browser-based blocking extensions, which studies [15, 29, 16] have found to be effective to various degrees in blocking third-party trackers. However, while industry surveys [32, 18, 6, 3] have shown that users primarily adopt Ad blocker extensions for user experience (UX) benefits, we lack a comprehensive understanding of how and why users adopt various browser-based blocking extensions in the real world. To improve the privacy protections offered by blocking extensions, we need to better understand users' motivations behind adopting these extensions in the first place, their understanding of the online tracking ecosystem, and whether these extensions work effectively in shielding them against online tracking.

To answer these questions, we conducted two large scale online surveys with current users and non-users of three types of blocking extensions (Ad blockers, Tracker blockers and Content blockers) on Amazon Mechanical Turk (MTurk). We asked three research questions. First, how much do users understand online tracking, and does heightened knowledge about online tracking relate with users adopting such blocking extensions? We investigated this question through the lens of mental models, which prior research has shown influence attitudes and behaviors [20]. Second, do users consciously adopt various blocking extensions to protect themselves from online tracking? Knowing users' intentions can help us understand whether the extensions function to according to users' expectations and if privacy protections are a motivating factor in adoption. Third, when and how do users disable their extensions and accept being tracked? We asked this question because extensions can fail to distinguish between content and trackers, and consequently break websites, potentially forcing users to choose between online tracking protection and accessing content [29].

We have three main findings which both confirm and extend previous work:

1. First, our results show that blocking extension usage only weakly relates with an advanced understanding of online tracking in the real world. Indeed, current blocking extension users were able to better articulate certain aspects of online tracking but these differences were small—despite them having used these extensions for long periods of time. This supports findings from

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018.
August 12–14, 2018, Baltimore, MD, USA.

previous research [37] studying first-time users of these extensions in a lab setting.

2. Second, we report evidence to confirm the expected: most Ad blocker users adopt these extensions primarily to improve their UX on the web and not to block online tracking. On the other hand, tracker blocker users adopt these extensions primarily to block online tracking. However, in an unexpected and new result, we found that most Content blocker users also adopt these extensions primarily to improve their UX on the web as opposed to block online tracking.
3. Third, our results show that current users report that they rarely experience website breakages because of their blocking extensions. However, when blocking extensions break websites, about half of all users disable their extensions so that they can access the content they desire. Their decision to give up tracking protection is based on the perceived value and importance of the content they are obstructed from accessing.

Based on our findings, we make the following recommendations. First, given users' lack of understanding of online tracking, we suggest that system designers should focus their efforts on building systems that automatically enforce tracking protection as opposed to having users take action to protect themselves (such as by installing an extension). We argue that browser vendors can play an important role in facilitating this type of default privacy protection. Second, we suggest that blocking extensions can be further improved by better understanding how website developers embed third-party trackers and deliver content through their websites so that non-use (disabling) is not forced upon users.

2. RELATED WORK

In this section, we touch upon relevant research on online tracking, use of different types of browser-based blocking extensions to prevent online tracking, and studies examining the usability and effectiveness of these extensions.

2.1 Online Tracking

When people visit a website, they interact with a *first* party and often, several *third* parties. The first party is the website or service people visit and intend to use, while third parties are embedded services and trackers that people indirectly and inadvertently interact with. First parties typically include third-party trackers to collect analytics about their customer base, show targeted advertisements, or to include functionality such as social media sharing links [36]. As an example, when someone visits The New York Times (NYT) website[1], the first party is The New York Times—the website that people directly interact with—and one of the third parties—at the time of writing this article—is Google Tag Manager[2], which provides the NYT with analytics about their visitors and marketing support. Another such third-party on the NYT website is Google Publisher Tags[3], which serves the NYT with targeted advertisements—often called Online Behavioral Advertising (OBA)—that are based on peoples' interests, demographics and browsing histories.

Extension Studied	Blocking Method
Ad blockers	
AdBlock	EasyList, EasyPrivacy (Not default)
AdBlock Plus	
Tracker blockers	
Ghostery	Ghostery Blocklist
PrivacyBadger	Heuristics
Disconnect	Disconnect Blocklist
Content blockers	
uBlock	EasyList, EasyPrivacy, Misc. lists
uBlock Origin	

Table 1: Summary of the browser-based blocking extensions considered in this study.

People do not directly interact with third-party trackers and are often oblivious of their presence yet they are still susceptible to data collection—so this type of tracking is considered privacy violating [26]. For instance, third-party trackers embedded across websites can *see* people visiting those websites, and link these websites visited to reconstruct peoples' browsing histories, which may contain sensitive websites people visited. Further, by just visiting certain websites people can reveal sensitive information including their interests, demographics, as well as the machines and devices they use. In the previous example, both third-parties on the NYT are tracking in nature, and they collect information about people and their activities as people visit websites where the same third-parties are embedded.

Third-party trackers are able to track people by largely employing *stateful* tracking, which involves the use of HTTP cookies to track website visits. However, some trackers have been shown to also engage in more *persistent* and *stateless* tracking techniques such as re-spawning Flash cookies and fingerprinting respectively—both of which can track people even when they clear HTTP cookies [13, 36]. In fact, when Flash cookies were first discovered [42] in 2009, it led to an FTC lawsuit [41].

2.2 Perceptions of Online Tracking

Previous studies [46, 2, 40, 22, 49, 25, 8, 27, 24, 35, 28] have examined peoples' perceptions of, and preferences towards data collection and advertising. For example, one study [22] explored peoples' mental models of how the Internet works, as well as their online privacy and security attitudes and behaviors. The authors found that people with stronger technical backgrounds were able to more clearly articulate privacy and security threats but took no additional steps to protect their privacy and security than people without a technical background. Another study [35] showed that people reported greater concern about data aggregation through third parties than first parties.

One set of these studies examined peoples' perceptions towards online tracking driven OBA. These studies have shown that peoples' attitudes towards OBA are nuanced. First, people find OBA desirable in certain situations (e.g., when a useful product is shown) but not in others (e.g., seeing negative and embarrassing online advertisements) [46, 2]. Second, peoples' attitudes toward OBA depends on how their data is being used [25, 24, 8]—the sensitivity of the data, how long it was retained, the type of advertisements it

[1] https://www.nytimes.com

[2] https://www.google.com/analytics/tag-manager/

[3] https://developers.google.com/doubleclick-gpt/

was used to deliver, and whether people had the necessary tools to control the advertising if they desired—to target them. Third, peoples' willingness to be tracked varies by the purpose of the tracking [28]—such as OBA, price discrimination, and customization—the entity tracking them (first party vs. third party), and the type of information being tracked (health, financial, or social).

Researchers have also shown that people often have misconceptions about how OBA and online tracking works. First, people have varying mental models about how their data is collected for targeting [49] and this influences their attitudes towards OBA. For instance, people who believed browsers store information used for targeting (e.g., through cookies) were more comfortable with OBA than those who did not; some people in this latter group believed they could use browser settings to clear that information and therefore, restrict OBA. In another instance [46], some people believed they could stop behavioral targeting by using anti-virus software on their machine, or by just using features in their browsers. Finally, researchers have found that people often confuse privacy and security [40], are unsure how tracking works, and therefore cannot adequately protect themselves.

2.3 Blocking Extensions

Currently, people can protect themselves against such tracking by using various browser-based blocking extensions, which take different approaches to block third-party trackers from loading and executing content. Informally, these extensions can broadly be classified into three types: Ad blockers, Tracker blockers, and Content blockers. Table 1 summarizes the extensions we considered in this paper.

2.3.1 Ad blockers

Ad blockers block advertisements from websites. Popular Ad blockers include AdBlock [1] and AdBlock Plus [33]. Both these extensions function using the EasyList [11] list, which contains several patterns corresponding to known advertisements. Each time a user's browser makes a request that matches a pattern in the list, these extensions block that request from loading.

Because Ad blockers block advertisements, they also block third-party advertisers that serve targeted advertisements, such as Google Publisher Tags on the NYT website. However, Ad blockers such as AdBlock and AdBlock Plus fail to block several other non-advertising third-party trackers unless they are specifically configured to do so. Both these Ad blockers can be augmented to block these non-advertising trackers by enabling other lists (e.g., EasyPrivacy [12]).

2.3.2 Tracker blockers

Tracker blockers block third-party trackers more generally, not just those that serve targeted advertisements. Different Tracker blockers take different approaches to blocking trackers. For instance, rather than using the EasyPrivacy ruleset, extensions such as Ghostery [17] and Disconnect [10] use internal lists maintained by the companies that built these extensions, which contain patterns corresponding to tracking services. Each time a user's browser makes a request that matches a pattern in these lists, these extensions block that request from loading. Other Tracker blockers such as PrivacyBadger [34] use heuristics to determine if a third-party is a tracker.

2.3.3 Content blockers

Some blocking extensions aim to function as general-purpose blockers, and block both advertisements and trackers embedded on websites. We call these extensions Content blockers to distinguish these blockers from those described above. Popular Content blockers include uBlock [44] and uBlock Origin [45]. Both these particular blockers have EasyList and EasyPrivacy enabled by default, along with other malware domain lists.

2.4 Effectiveness of Blocking Extensions

Numerous studies have measured the effectiveness and performance of various Ad, Tracker and Content blockers across websites using standard web automation tools [5, 47, 13, 29, 16, 15]. For instance, research by Balebako and colleagues [5] examined the effectiveness of two different privacy tools—Ghostery and Targeted Advertising Cookie Opt-Out (TACO)—in limiting OBA. They tested how the content of online advertisements varied based on the initial profile they were viewed with and when the browser is/is not configured with the extension in question, and found that both types of blocking extensions limit OBA successfully.

Other studies [13, 29, 16, 15] have examined the effectiveness of Ad blockers and Tracker blockers in limiting the number of third-party requests made by websites. These studies collectively found that extensions are effective to varying degrees. For instance, extensions that work with pre-compiled lists such as Ghostery and Disconnect perform better in limiting third-party content than heuristic-based extensions like PrivacyBadger, but overall many extensions miss less prevalent third-party trackers, i.e., trackers found on fewer websites. While these studies show that these extensions are indeed effective in blocking online tracking, they do not examine whether users consciously adopt these extensions to block online tracking, and how effectively these extensions work from a user point-of-view.

2.5 User Studies of Blocking Extensions

Several industry surveys [32, 18, 6, 3] have examined users' motivations behind adopting Ad blocker browser extensions. Collectively, these surveys found that most users adopt these extensions for user experience reasons such as to remove intrusive advertisements and reduce clutter on websites. However, these report findings do not always agree which is why our work examines these topics in more detail. For instance, PageFair [32] found that nearly one third of all their participants used Ad blockers for security benefits, in contrast to global web index [18] and HubSpot [3], which found that nearly one third of users used Ad blockers for privacy benefits, such as to shield their information from advertisers.

Some studies [23, 37] have conducted lab-based usability research on browser-based blocking extensions. First, in a lab study, Leon and colleagues [23] examined whether first-time users could successfully opt-out of or block OBA using AdBlock Plus and Ghostery. They found that users face several problems when dealing with both extensions—including confusing interfaces and technical jargon—that limit their ability to reduce exposure to OBA. Likewise in a lab study, Schaub et al. [37] found that exposing first-time users to Tracker-blocking extensions heightened their awareness of online privacy; however, users found it difficult to fully understand how they were being tracked and what the consequences of being tracked were.

These studies shed important insights into the usability of these extensions, but they either only considered Ad blocker extension users and were not peer reviewed, or only considered a small sample of first-time users interacting with these extensions for the duration of a lab study. In our study, we examine a much larger sample of *real* users of these extensions, who have adopted and currently use these extensions. We also consider a wider variety of extensions including Ad blockers, Tracker blockers, and Content blockers. Further, understanding whether these users' knowledge of these extensions relates with greater use of these extensions in practice, whether users consciously adopt these extensions to protect themselves against online tracking, and how effectively these extensions protect users still remains unclear. In this paper, we examined these questions using both surveys and actual measurements to help determine how we can improve protections against online tracking.

3. METHOD

We conducted two surveys on MTurk. In our surveys, we studied three categories of blocking extensions: Ad blockers, Tracker blockers, and Content blockers, which are listed in Table 1. Through the first survey, we answered two research questions. First, to better understand whether and how users' mental models about online tracking are related to blocking extension adoption, we asked what users and non-users understand about online tracking. Second, to better understand if users are adequately protected from online tracking and to design better tracking protections, we investigated whether whether users consciously adopt these extensions to prevent online tracking. We administered a second survey to all participants from the first survey who reported using at least one blocking extension to answer our third research question: when these extensions break websites, we asked how and whether users decide to disable their extensions, and consequently accept being tracked.

3.1 Survey Design and Deployment

We describe the design of our two surveys below. The study was approved by the Institutional Review Board of our university. The Appendix contains both of our surveys.

3.1.1 Survey One

Questions: The first survey contained four parts and included both open and closed-ended questions. In the first part of the survey, we asked about participants' general Internet behavior. We asked participants how much time they spent online, what services they used, and how many and which Internet connected devices they had access to. In the second part, we gathered participants' general awareness about *Internet/Web tracking*, whether they had heard of this term, who they thought collected information about them as they browsed the Internet, what information they thought was collected, and if they had taken any steps to limit their tracking. In the third part of the survey, we gathered data about the blocking extensions participants had installed on their current browsers. We asked participants whether they had any of the Ad blockers, Tracker blockers or Content blockers listed in Table 1 installed on their current machines, and for each reported blocking extension, we asked who installed it, how long had they been using it, how they learned about it, and why they used it. To collect participants' reasons for adopting their extensions, we used both open and closed-ended responses. Participants first provided their reasons in an open-ended format, after which we asked them to respond to a set of statements (see Appendix A.18.g)—which we borrowed and edited from related work [23]—on a five-point scale ranging from strongly disagree to strongly agree.

Finally, in the fourth part of the survey, we gathered participants' demographic information, including age, gender, education, and profession.

Measurements: In addition to the survey questions, we conducted several measurements of participants' browser configurations and privacy settings to confirm what they self-reported. We checked whether participants' browsers were blocking third-party cookies from being set, blocking third-party trackers, and blocking advertisements.

To measure whether participants' browsers were blocking third-party cookies, we attempted to set and read back a cookie from a different domain than our survey. This domain was also under our control and resolved to a server hosted at our university.

To measure whether participants' browsers were blocking third-party trackers—indicating the presence of an extension that blocked such trackers (such as by using EasyPrivacy)—we added the Google Analytics tracker to the survey and detected whether its JavaScript objects correctly loaded. We chose the Google Analytics tracker for two reasons. First, it is a common tracker, blocked by the extensions we considered, and therefore a good choice to run measurements. Second, we did not want to cause any harm to participants' by exposing their data to possibly nefarious trackers. The Google Analytics account we used for this purpose was password and two-factor protected, and under our control.

To measure whether participants' browsers were blocking advertisements—indicating the presence of an extension that did so—we injected an image wrapped in a HTML div element tagged with a HTML tag found in EasyList into the survey, and checked whether its element loaded.

3.1.2 Survey Two

Questions: We sent survey invites to participants from the first survey who had reported using at least one of the extensions listed in Table 1. This survey asked participants to report their experiences when they had to disable their extensions in order to access content in two particular situations. First, when websites fail to function correctly as a result of users' extensions, and second, when websites ask users to disable their extensions in order to access content (as others have measured [29]). In the first part, we asked participants whether they had experienced website fail to function correctly as a result of their blocking extensions; if they responded yes, we further asked them to list the name and type of the websites(s) they experienced break, and how frequently they experienced such breakages. We then asked participants how they responded in the past after experiencing such breakages, whether they proceeded to attempt to fix the websites, and what if, any steps they took to fix the websites. The second part of the survey closely mirrored the first; instead of the asking about incorrectly functioning websites, we asked users to recollect whether they had seen Ad-blocking messages that appeared as a result of their blocking extensions. Both parts appeared in random order. In this paper we do not report results from the Ad-blocking messages section of the survey.

3.1.3 Two-Step Survey Design

We designed and launched the surveys in two phases for two reasons. Since survey one asked participants to identify their reasons for adopting blocking extensions, we did not want these reasons to prime them when they were later asked to describe their experiences when disabling their extensions. Second, we were concerned that merging both the phases would make the survey long enough that it would be difficult for participants to complete in one sitting.

3.1.4 Survey Pilot

Before launching the surveys, we conducted a small-scale pilot data collection to ensure the questions were comprehensible and clear. This practice, called cognitive interviews [43], is common in survey design and development. We launched our survey on UserBob[4], a crowd-sourced usability testing website, and invited 10 participants to complete the survey. Participants were asked to "think-aloud" as they completed the survey, specifically highlighting what each question meant to them and what specific information each question was soliciting. Participants captured their screens in a video while taking the survey and thinking-aloud. We used these results to refine and revise our questions. These screen captures lasted for about 20 minutes, and we paid participants $10 each.

3.1.5 Survey Deployment

We used the MTurk platform to recruit participants. We launched the first survey in May 2017, and paid participants $1.00 for completing the survey. We advertised the survey as a "Tell us about your Internet browsing experience" task to mask the survey's purpose and reduce response bias. We required that Turkers be 18 or older, located in the United States (US), and have an approval rating of 95% or higher in order to qualify to take the survey. The survey took between 10-15 minutes to complete.

Three weeks after the first survey, we launched the second survey in June 2017 as a bonus task to all the participants who took the first survey and had been using a blocking extension. We paid participants $2.00 to complete this survey, which took no longer than 10 minutes to complete.

We specifically chose MTurk since its capabilities allowed us to re-target the same participants for the second survey survey. Further, since MTurk participants are known to be more Internet savvy than other Internet users, we were also likely to find a larger pool of blocking extension users compared to other platforms.

3.2 Participants

We recruited 1000 participants from MTurk; participant demographics are summarized in Table 2. Two-thirds (N = 664) of participants from survey one had at least one Ad blocker, Tracker blocker, or Content blocker installed. Nearly half of all participants were aged between 18-34 and the sample was nearly equally split in terms of gender with a slightly higher male participation. Close to two-thirds of the sample had attained a college degree. Finally, the median annual income ranged between $35,000 and $49,999. A logistic regression modeling users vs non-uses of these extensions revealed age ($O.R. = 0.97$, $p < 0.00001$) and gender [Male] ($O.R. = 2.45$, $p < 0.00001$) as significant predictors, indicating that current users were more likely to be younger and male. We sent the follow-up survey invitation to all participants from Survey One, and 480 ($\sim$ 72.3%) subsequently completed Survey Two.

Demographic	All Participants	Extension Users
Age		
18–24	14.0%	17.8%
25–35	45.1%	48.8%
36–45	21.8%	17.6%
46–55	11.0%	9.0%
>55	8.1%	6.9%
Gender		
Male	53.1%	60.7%
Female	46.2%	38.6%
Other	0.7%	0.8%
Education		
No High School	0.2%	0.3%
High School	10.9%	10.2%
Some College	28.8%	28.0%
Bachelor's	37.8%	40.4%
Associate's	12.4%	12.5%
Master's	7.5%	6.6%
Other	2.4%	2.0%

Table 2: Demographic information of the survey participants (N = 1000) and the browser-based blocking extension users (N = 664).

3.3 Data Analysis

For qualitative analyses of open-ended responses, the first author examined the data and first created a codebook. The research team held regular meetings to discuss the initial codes and arrived at the final set of codes after several iterations of discussions and consensus building. We used the finalized codebook to code the open-ended responses. Next, we grouped and organized these codes into themes [38] where applicable. As an example, grouping participants' responses around how tracking took place resulted in codes *use_cookies*, *use_searches*, *use_online_activities*, and *use_clicks* among others. For quantitative analyses, we provide summary statistics, and using Chi-squared tests of proportions, compared sub-populations (users vs. non-users).

4. FINDINGS

In the following section, we summarize our findings from both surveys.

4.1 Blocking Extension Usage

Figure 1 presents the distribution of the blocking extension categories across the participants. Of the 664 participants who reported using at least one blocking extension, Ad blockers were the most prevalent (512 of 664 $\sim$77%), followed by Content blockers (205 of 664 $\sim$31%), and finally, Tracker blockers (84 of 664 $\sim$13%). Users sometimes had one or more blockers, a pattern which was particularly striking in the context of Tracker Blockers: nearly 90% of all Tracker blocker users additionally used either an Ad blocker

[4] https://userbob.com/

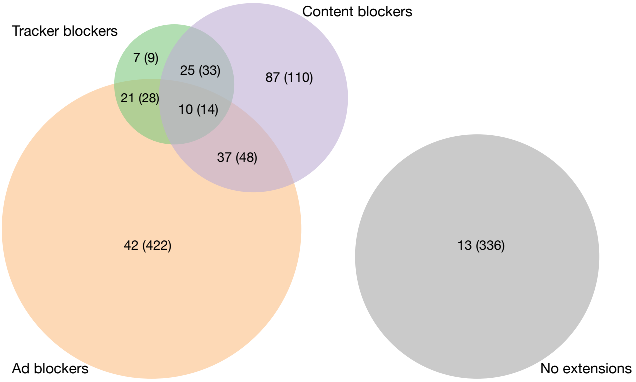

Figure 1: Venn diagram showing the distribution of N = 1000 participants' self reported usage of blocking extensions (within braces) versus those we measured to be blocking third-party trackers (outside braces). For example, only 42 of 422 users who self-reported using *only* Ad blockers were measured to be blocking trackers.

or Content blocker or both.

Using scripts embedded in our survey, we also measured whether participants were blocking third-party trackers and cookies. Across our sample, 9.2% of participants were blocking third-party cookies; a little less than a quarter (242 of 1000) of all participants were blocking third-party trackers. Across extension types, we noted that only about one-fifth of all Ad blocker users (110 of 512 ∼22%), three-quarters of all Tracker blocker users (63 of 84 ∼75%), and three-quarters of all Content blocker users (159 of 205 ∼77%) were blocking third-party trackers.

While our measurements do indicate that most users who reported using these extensions were actually using them, they do not paint a perfect match with the self-reports. We speculate a number of potential reasons for this finding. First, users of Ad blocker extensions such as AdBlock and AdBlock Plus may not have enabled EasyPrivacy, which blocks Google Analytics. Second, users may not have not enabled full protection mode for Ghostery and may not have blocked Google Analytics—the tracker we used to measure tracker blocking. Third, PrivacyBadger does not, by default, block Google Analytics, the tracker we used in our measurements, as it considers it to be a first-party tracker. Fourth, some participants may be using less popular extensions we did not explicitly list. Finally, our measurement script returned incomplete data for certain users due to measurement error: our measurement server was inaccessible momentarily during the survey.

Averaged across the extensions, most users reported learning about these extensions from Internet articles (34.1%) or social media (19.9%). Close to two-thirds (62.5%) of users reported using these extensions on a browser other than the one they took the survey on on their devices, and less than half (40.2%) reported using these extension on a different device than the one they took the survey on, on average. All users had been using them for at least a "A few years" (median across each extension type).

4.2 Mental Models of Online Tracking

To understand participants' mental models of online tracking and whether more developed mental models related with adopting blocking extensions, we analyzed users' (U) and non-users' (NU) mental models together, highlighting instances where these two groups agreed or disagreed. We analyzed the data that emerged from the open-ended question for this section. To compare differences between the groups, we the used chi-square test of proportion. We corrected for multiple testing using the False Discovery Rate method [7], which led to our new significance threshold of 0.025. Table 3 summarizes the themes we list below.

4.2.1 Users & Non-Users Have Like Understanding

Participants' understanding of the online tracking ecosystem could be broken down into four categories: knowing the entities that participated in online tracking, understanding the information that was collected by these entities, recognizing the outcomes of online tracking, and comprehending how online tracking occurred.

Entities that Track. Across our participants, a majority believed advertisers (78.9%) and websites they visited (73.1%) engaged in online tracking. We found no evidence to suggest that the frequency of mention of both entities differed significantly between users and non-users (advertisers: $U = 80.3\%$, $NU = 76.1\%$, $\chi^2 = 2.4$, $p = 0.12$; websites: $U = 74.3\%$, $NU = 70.7\%$, $\chi^2 = 1.5$, $p = 0.23$). This suggests that both users and non-users were equally well-aware of advertisers and websites they visited as entities that tracked them.

Less than 15% of participants mentioned that they were tracked by government agencies ($U = 13.7\%$, $NU = 8.7\%$, $\chi^2 = 5.3$, $p = 0.02$), Internet Service Providers/ISPs ($U = 6.7\%$, $NU = 3.5\%$, $\chi^2 = 4.3$, $p = 0.04$), and third-party companies ($U = 3.9\%$, $NU = 1.1\%$, $\chi^2 = 6.1$, $p = 0.01$). While the frequency of mention of both government agencies and third-party companies differed significantly between users and non-users, these entities were mentioned infrequently by our participants. This suggests that overall far fewer participants were aware of the government, ISPs, and third-party companies as entities that tracked them.

Information Tracked. Only a small fraction of participants (3.7%) did not explicitly list any information that was tracked about them. Well over half of all participants (58.8%) mentioned that basic information was tracked about users, including their demographics, name, sex, email address, location, likes and dislikes, and habits. We found no evidence that users and non-users differed significantly in listing this type of information ($U = 61.2\%$, $NU = 56.3\%$, $\chi^2 = 2.2$, $p = 0.14$), suggesting that both groups were aware that information about them could be tracked.

More than half the participants (54.8%) felt that information about users' online activities such as websites visited, time spent on websites, products looked at and clicked on, search and purchase histories was tracked. We found no evidence that current users and non-users differed significantly in mentioning this type of information ($U = 55.9\%$, $NU = 53.6\%$, $\chi^2 = 0.48$, $p = 0.49$), suggesting that both groups were mostly aware that information about their activities could be tracked.

Themes	**Total (%)**	**Users (%)**	**Non-Users (%)**	**Difference (%)**	**p-value**
Entities that Track					
Advertisers	78.9	80.3	76.1	4.2	0.12
Websites Visited	73.1	74.3	70.7	3.6	0.23
Government Agencies	12.0	13.7	8.7	5.0	**0.02**
Internet Service Providers	5.6	6.7	3.5	3.2	0.04
Third-Party Companies	3.0	3.9	1.1	2.8	**0.01**
Information Tracked					
User Attribute Information	59.6	61.2	56.3	4.9	0.14
Behavioral Activities	55.1	55.9	53.6	2.3	0.49
Device Information	26.1	32.9	12.6	20.3	**<0.0001**
Outcomes of Tracking					
Visible Outcomes	44.9	46.7	41.2	5.5	0.10
Invisible Outcomes	23.9	33.2	5.5	27.7	**<0.0001**
Tracking Mechanisms					
Through Activities	56.1	57.7	52.9	4.8	0.4
Through Cookies	23.9	29.7	12.3	17.4	**<0.0001**

Table 3: Summary of the themes that emerged from participants' mental models of online tracking broken down by users and non-users. Bolded p-values are significant at the 0.025 level.

Approximately a quarter (26.1%) of all participants mentioned that information about Internet users' devices, such as their browser name and version, and IP address was tracked. However, current users mentioned this information significantly more often than non-users (U = 32.9%, NU = 12.6%, $\chi^2 = 47.6$, $p < 0.0001$). This suggests that blocking extension users were more aware than non-users about the information that was tracked about their devices. Overall, over half of all participants were aware that tracking occurs but a significant number of participants did not know that online activities and devices could be tracked.

Outcomes of Tracking. A little more than half of all participants (57.4%) were aware of at least one outcome resulting from online tracking. Participants described both "visible" and "invisible" outcomes as others have previously classified [28]. Visible outcomes included those that users could observe in their browsing experience (e.g., targeted advertising). Invisible outcomes included those that users could not directly observe (e.g., price discrimination).

More specifically, less than half of all participants (∼44%) cited visible outcomes of online tracking such as targeted advertisements, customization of websites, and deciding what to sell to users. We found no evidence that current users and non-users differed in how frequently they brought up this outcome (U = 46.7%, NU = 41.2%, $\chi^2 = 2.7$, $p = 0.10$). This suggests than while both groups were equally aware of tracking outcomes they could directly observe, the majority of participants did not even recognize visible outcomes of tracking as tracking-related.

Even fewer participants (19.4%) reported invisible outcomes of online tracking, including companies maximizing their revenue, offering varying prices, and collecting personally identifiable information. Blocking extension users brought up this outcome significantly more often than non-users (U = 33.2%, NU = 5.5%, $\chi^2 = 94.0$, $p < 0.0001$). This suggests that extension users were more aware of outcomes of online tracking they could not directly observe than non-users. Still, only close to a third of blocking extension users and less than one-fifth of all participants reported knowing these outcomes. Overall, most participants in our study were not able to easily recognize signs of online tracking.

Tracking Mechanisms. Participants varied in how they believed tracking worked. Slightly more than half the participants believed that online tracking occurred on websites through their activities on the websites, the products and advertisements they clicked on, or their search and product history. We found no evidence to suggest that this belief varied significantly between current users and non-users (U = 57.7%, NU = 52.9%, $\chi^2 = 0.7$, $p = 0.4$). This suggests that both groups were aware that their activities on websites could be tracked.

A smaller fraction of participants (25.5%) stated that cookies were the underlying mechanism through which tracking occurred, and this number varied significantly between current users and non-users. In particular, current users mentioned cookies three times more than non-users (U = 29.7%, NU = 12.3%, $\chi^2 = 37.2$, $p < 0.0001$). This suggests that users were more aware than non-users that cookies can be the underlying mechanism through which tracking works; however only about one-third of users mentioned this overall. The majority of our participants were aware that tracking could occur by collecting information about online activities but three quarters of all participants were not aware that cookies could be used for tracking.

4.2.2 Comfort with Tracking Depends on Context

We examined both users' and non-users' responses with respect to how comfortable they were with their data being collected on the Internet. Confirming results from previous work on users' and attitudes towards data collection [46, 2, 28, 39], we found that participants' level of comfort was context dependent: both current users and non-users described situations where they were comfortable and uncomfortable with data collection. The majority of all users were not comfortable with tracking in general. A little over half users (55.4%) and a little less than half non-users (45.9%) were uncomfortable with their data being collected, harboring a general mistrust toward companies that collect data about them, and wanting to keep their information and activities private. These participants often expressed apathy, saying that data collection was hard to stop, and that if companies really wanted their data, they could acquire it in different ways. These numbers differed significantly between users and non-users ($\chi^2 = 8.1$, $p = 0.005$).

By contrast, a little over a quarter of users (28.5%) compared to more than one-third non-users (36.4%) were comfortable with their data being collected ($\chi^2 = 6.5$, $p = 0.011$). Both sets of participants cited several reasons for being comfortable with tracking such as when the online tracking resulted in positive gains, such as receiving special deals through targeted advertising. For others, tracking was acceptable because they had nothing to hide, and that they believed online services needed users data in order to offer services and function for free.

To summarize, we found that most participants—regardless of whether they used a blocking extension—had only a basic understanding and awareness of online tracking. Our findings support and extend findings from prior work in lab settings that users may know a little, but not significantly more about online tracking after using a browser-based extension [37, 23]. We show that fewer participants were aware of entities that tracked them other than the ones they could explicitly see provide visible modification to content. Across both users and non-users, there existed some differences: users were slightly more able to articulate what data about users' devices is collected, the invisible outcomes of tracking, and how cookies are used in tracking than non-users. However, these differences were spread across only a third of the sample of extension users in each case, indicating that despite these differences, extension users did not present elevated knowledge and understanding about online tracking even after using these extensions for many years.

4.3 Why Use Blocking Extensions?

We examined whether users consciously adopted blocking extensions to block third-party trackers. In the survey, we solicited participants' reasons behind adopting their extensions both in the form of open and closed responses. To analyze the close responses, we binned the Likert scale measurements into agree, not sure, and disagree bins. We compared the open and close ended responses and noted any similarities and differences. We found that current users' responses from the open responses could be grouped into three primary reasons for extension adoption: user experience improvements, security, and privacy—similar to the options we offered them to select from the closed responses.

4.3.1 UX Reasons Drive Ad, Content Blocker Users

In the open responses, the most common reason users cited for adopting Ad blockers and Content blockers was to improve their user experience when browsing the Internet, with the latter finding being unexpected. Close to 89% of participants who used Ad blockers and 84% of participants who used Content blockers said they were motivated by user experience improvements. On the other hand, only a small fraction of users (11.9%) reported using Tracker blockers for user experience improvements. Current extension users' elaborated three main reasons:

Reducing clutter. Nearly half of all current users (50.5%) reported using blocking extensions to block the clutter on webpages. For instance, participant P716, an AdBlock Plus user, stated: *"I hate advertisements that affect my ability to navigate a page without distraction, so I choose to block them in order to have a faster, more streamlined experience."* Often for such users, the extensions were a means to help them block advertising content that obstructed them from viewing desired content on a website.

Blocking Pop-ups. Two-fifths of all current users (40.2%) reported using these extensions to specifically block advertisements that appeared as pop-ups on webpages, which users considered intrusive in nature. For instance, participant P900, an AdBlock Plus user, said: *"The popup advertisements interfere with my online experience. They are annoying and slow down my computer. AdBlock Plus allows me to circumvent unsolicited advertisements."*

Speedup Loading Times. Finally, one-third of all current users (33.1%) reported they used these extensions to speed up the loading of websites, which consequently help them conserve their data and bandwidth. For instance, participant P458, an uBlock Origin user, commented: *"[I use it] to prevent the 100s of advertisements that appear when browsing sites. So many advertisements play or are shown that it slows down browsing performance and uses more bandwidth."*

In agreement with the open responses, ∼95% of both Ad blocker and Content blocker users reported using these extensions for user experience reasons in the close ended responses. We also noticed an additional (∼65%) Tracker blocker users reported using their extensions for user experience reasons.

4.3.2 Privacy Reasons Drive Tracker Blocker Users

Looking at the open responses, 76% of Tracker blocker users said they primarily used the extensions to protect their information from third-parties and advertisers. Participants were concerned that advertisements networks and data mining companies on the Internet collected their data, tracked their browsing history, and showed them targeted advertisements. They believed that they could, using these extensions, block companies that engaged in such practices. For instance, participant P899, a Ghostery user, stated: *"I use Ghostery so advertisers and sites will not track my information or collect info using cookies."* On the other hand, only a small fraction of participants who used Ad blockers (7%) and Content blockers (10%) used them for privacy reasons. In agreement with the open responses, ∼90% of Tracker blocker users reported using these extensions for privacy reasons in the close ended responses. We also noticed an additional Ad blocker (∼76%) and Content blocker (∼71%) users reported using their extensions for the same privacy reasons.

4.3.3 Fewer Security Reasons Across Extensions

From the open responses, only ∼10% of participants—across Ad blocker, Tracker blocker, and Content blocker users—stated they used these extensions for security reasons. Those who did use these extensions for security noted they used it in order to prevent harm to their devices from malicious advertisements and scripts online. For instance, participant P450, an AdBlock user, elaborated: *"I use Adblock because of all the EXCESSIVE advertisements/popups that end up causing me to click on something that I'm not wanting to click on and then a pop-up comes up alerting me that my computer has a Virus, telling me to call some number. Let's just say those people really irritate me."* On inspecting the close responses, this number increased. We noticed additional users across all extensions—Ad blockers (56%), Tracker blockers (39%), and Content blockers (62%)—reported using their extensions for the same security reasons.

Overall, we noted participants associated each extension type with a primary and secondary reason for adoption, which emerged from the open and close ended responses respectively. That is, users may have mentioned their primary reasons for using the extensions as opposed to including secondary reasons in the open ended responses. Even though users may be aware of other benefits from these extensions, their primary motivation is more focused: Ad blockers and Content blockers primarily for user experience gains, and Tracker blockers primarily for privacy reasons.

4.4 Dealing With Broken Websites

We specifically studied users' experiences when blocking extensions broke the functionality and appearance of websites, as other studies have tried to capture using instrumented measurements [29]. We examined specific changes users reported about their interface and browsing activity, how frequently they experiences these breakages, and users' decision making with respect to disabling their extensions.

4.4.1 Users Report Limited Breakages

Only about two-fifths (180/480) of participants who took the second survey had experienced at least one website that failed to function correctly because of their browser extensions. The majority (94.6%) of those who reported broken website experiences observed them *rarely* or *sometimes* in the span of any given week. Participants reported the following experiences with their extensions in decreasing order of prevalence:

1. Webpages failed to load completely and the content failed to appear (28.7%)
2. Embedded videos failed to play (24.3%)
3. Webpages appeared distorted, and the elements looked out of place (13%)
4. Pop-ups that drove functionality failed to appear (8.1%)
5. Images failed to load completely (7.5%)

Overall, users' self-reported website breakages were lower than expected, which suggests that the blocking extensions were largely effective in distinguishing between trackers and content. However, given that websites failing to appear completely, and videos failing to play, were amongst the most commonly cited website breakages suggests that these extensions often confused trackers and Content Distribution Networks [29].

4.4.2 Content and Trust Drive Disabling Decisions

When websites failed to function correctly, nearly half the users (91/180) who experienced such breakages stated that they never attempted to fix and access the website when they experienced them break, and instead ignored and went on to find alternate content. The other half (89/180) who did access the content on such websites—either sometimes or always—by disabling their extensions based their decisions on the following criteria:

Value of Content. Users who stated they sometimes or always attempted to access the content of such websites, based their judgment on the uniqueness and importance of the content they intended to view; that is, could they gain access to the same content elsewhere? Participant P107 best illustrates this point: *"It depends if I really want to access the content, but I usually just navigate away."*. This suggests breakages can certainly dissuade users from using certain sites if the content is not perceived as unique.

Trust in Website. Similarly, users who stated they sometimes or always attempted to access the content of such websites, reported accessing content if they "trusted" the website and if it was familiar to them; that is, had they accessed it before? Participant P282 explained: *"If it's a site I trust, and understand why they need access to cookies, JavaScript, etc. I will attempt to relax the permissions so the site will work. Otherwise I look for an alternative site (and there's almost always an alternative!)."* This suggests that less popular websites which cause breakages can lose content consumers if blocking extensions do not interact well with their websites.

Overall, most participants reported only limited breakages in the span of a given week, indicating that these blocking extensions largely work effectively from the user point of view. However, when websites did break, nearly half the users attempted to fix the websites by disabling their extensions—and therefore gave up their protection—and based their decisions on how much they valued the content on and the trust they had in the website.

5. DISCUSSION

In this section, we discuss the broader implications of our findings, and outline directions for future work.

5.1 Reducing Privacy Protection Burden

First, our results show that despite having some knowledge about online tracking and how it worked, participants remained mostly uninformed. Having a browser extension did not significantly relate with having a more developed mental model of online tracking. Having adopted these extensions, users remained protected from online tracking to the degree supported by the extensions in their default modes. While these defaults were largely configured correctly for Content blockers and Tracker blockers, they were less so for the largest extension category in our dataset: Ad blockers. Indeed, we saw that only about 10% of all Ad blocker users had enabled EasyPrivacy, which continued to remain disabled by default.

Therefore, we suggest that asking users to take action to protect their privacy may be a sub-optimal suggestion. Instead, an alternate proposal for enhanced privacy protection is to pull users out of the equation completely, and design systems that protect users automatically. Echoing the call of others [22, 31], we suggest that browser designers could more successfully protect users from online tracking through defaults (e.g., by restricting third parties' access to user data), rather than requiring users' to take proactive, intentional steps such as adopting a browser-based blocking extension. In fact, several browser vendors have moved in this direction recently. For example, Mozilla recently incorporated online tracking protection into their private browsing mode, meaning that users who switched to private browsing would be protected from third-party tracking [30]. Apple took this a step further and implemented intelligent tracking restrictions in Safari 11 [4], where they restricted the lifetime of cookies set by third-party trackers and advertisers, thereby restricting how much data these trackers can collect about users. Future work could examine privacy enhancements that browsers can implement such as contextual situations—e.g. webpages where sensitive information is entered—where third-party trackers should explicitly blocked.

5.2 Reducing Blocking Extension Failure

Second, our results point out that browser-based blocking extensions work largely effectively from a user perspective. When websites did break, users noticed that embedded videos failed to play, or parts of the website failed to load completely. Future work could examine how well users' self-reports of website breakages match with actual website breakages in the wild. Doing so could help determine ways in which extensions can better support feedback from users to improve protection coverage. Out of the extensions we examined in this study, only Ghostery and PrivacyBadger currently collect any feedback at all.

When website breakages occur, users are required to disable their extensions and accept the trackers embedded on the website. Our study reveals that users only disable their blocking extensions when the content they attempted to access is valuable, or if they are familiar with and trust the website (e.g., from a previous engagement). To ensure that users are protected against online tracking—and that non-use is not forced upon them—requires building more efficient blocking tools. For instance, recent approaches to using machine learning to discriminate between JavaScript-based content serving and tracking content has been explored with high accuracy [19]. Improving the status-quo can also be achieved through a broader conversation between the various stakeholders including extension developers and publishers of websites. We encourage the SOUPS and broader privacy community to further investigate how publishers embed content and use third-party services, and the steps that can be taken to design better solutions that do not force users to disable their extensions.

6. LIMITATIONS AND FUTURE WORK

Out study is not without limitations. First, we used Mechanical Turk for data collection, and therefore findings are not generalizable to the full population of Internet users. Recent research has shown that adult Turkers in the U.S. have more privacy concerns than the regular adult US population [21]. Therefore, it is likely that the number of users of these extensions in the general population are much lower. Future research could examine the external validity of these findings in greater detail.

Second, we examined the results in the context of self-reported extension usage by users, but also measured extension usage to ensure users were actually using these extensions; while these measures were mostly in agreement, there were occasions where users reported certain extensions but we did not detect them. However, overall, users have been shown to be able to accurately self-report more deliberate actions, including external browser extension usage [48].

7. CONCLUSION

We studied real world use of blocking extensions to learn how to improve user protections against online tracking. Our results show that Ad blockers and Content blockers are more widely used than Tracker blockers. Furthermore, both users and non-users have limited mental models of online tracking, that they mostly adopt blocking extensions to improve their user experience, and that when extensions break websites, users disable the extensions based on how important the content they are accessing is to them. Based on our findings, we make recommendations to improve blocking tools and provide enhanced privacy by improved extension defaults to better protect users from online tracking.

8. REFERENCES

[1] AdBlock. Adblock. https://getadblock.com, 2017.

[2] L. Agarwal, N. Shrivastava, S. Jaiswal, and S. Panjwani. Do not embarrass: Re-examining user concerns for online tracking and advertising. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 8:1–8:13, New York, NY, USA, 2013. ACM.

[3] M. An. Why people block ads (and what it means for marketers and advertisers). https://research.hubspot.com/why-people-block-ads\-and-what-it-means-for-marketers-and\-advertisers, 2016.

[4] Apple. Apple. https://webkit.org/blog/7675/intelligent-tracking-prevention/, 2017.

[5] R. Balebako, P. Leon, R. Shay, B. Ur, Y. Wang, and L. Cranor. Measuring the effectiveness of privacy tools for limiting behavioral advertising. 2012.

[6] M. Bauman. Six surprising findings about ad block users. https://www.forbes.com/sites/forbesagencycouncil/2017/07/11/six-surprising-findings-about-ad-block-users, 2017.

[7] Y. Benjamini and Y. Hochberg. Controlling the false discovery rate: a practical and powerful approach to multiple testing. *Journal of the royal statistical society. Series B (Methodological)*, pages 289–300, 1995.

[8] F. Chanchary and S. Chiasson. User perceptions of sharing, advertising, and tracking. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 53–67, Ottawa, 2015. USENIX Association.

[9] ConsumerReports. Want to protect against websites that spy on you? get an ad blocker. https://www.consumerreports.org/digital-security/to-protect-against-websites-that-spy-on-you\-get-an-adblocker/, 2018.

[10] Disconnect. Disconnect. https://disconnect.me/, 2017.

[11] EasyList. Easylist. https://easylist.to/easylist/easylist.txt, 2017.

[12] EasyPrivacy. Easyprivacy. https://easylist.to/easylist/easyprivacy.txt, 2017.

[13] S. Englehardt and A. Narayanan. Online tracking: A 1-million-site measurement and analysis. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 1388–1401, New York, NY, USA, 2016. ACM.

[14] FTC. Online tracking. https://www.consumer.ftc.gov/articles/0042-online-tracking, 2018.

[15] K. Garimella, O. Kostakis, and M. Mathioudakis. Ad-blocking: A study on performance, privacy and counter-measures. In *Proceedings of the 2017 ACM on Web Science Conference*, WebSci '17, pages 259–262, New York, NY, USA, 2017. ACM.

[16] A. Gervais, A. Filios, V. Lenders, and S. Capkun. Quantifying web adblocker privacy. *IACR Cryptology ePrint Archive*, 2016:900, 2016.

[17] Ghostery. Ghostery. `https://www.ghostery.com/`, 2017.

[18] GlobalWebIndex. The state of mobile ad-blocking. `https://www.globalwebindex.com/reports/mobile-ad-blocking-2017`, 2017.

[19] M. Ikram, H. J. Asghar, M. A. Kaafar, A. Mahanti, and B. Krishnamurthy. Towards seamless tracking-free web: Improved detection of trackers via one-class learning. *Proceedings on Privacy Enhancing Technologies*, 2017(1):79–99, 2017.

[20] P. N. Johnson-Laird. Mental models and human reasoning. *Proceedings of the National Academy of Sciences*, 107(43):18243–18250, 2010.

[21] R. Kang, S. Brown, L. Dabbish, and S. Kiesler. Privacy attitudes of mechanical turk workers and the u.s. public. pages 37–49. USENIX Association, Submitted.

[22] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler. "my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 39–52, Ottawa, 2015. USENIX Association.

[23] P. Leon, B. Ur, R. Shay, Y. Wang, R. Balebako, and L. Cranor. Why johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, pages 589–598, New York, NY, USA, 2012. ACM.

[24] P. G. Leon, A. Rao, F. Schaub, A. Marsh, L. F. Cranor, and N. Sadeh. Privacy and behavioral advertising: Towards meeting users' preferences. In *Symposium on usable privacy and security (SOUPS)*, 2015.

[25] P. G. Leon, B. Ur, Y. Wang, M. Sleeper, R. Balebako, R. Shay, L. Bauer, M. Christodorescu, and L. F. Cranor. What matters to users?: Factors that affect users' willingness to share information with online advertisers. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 7:1–7:12, New York, NY, USA, 2013. ACM.

[26] J. R. Mayer and J. C. Mitchell. Third-party web tracking: Policy and technology. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 413–427. IEEE, 2012.

[27] A. McDonald and L. F. Cranor. Beliefs and behaviors: Internet users' understanding of behavioral advertising. 2010.

[28] W. Melicher, M. Sharif, J. Tan, L. Bauer, M. Christodorescu, and P. G. Leon. (do not) track me sometimes: Users' contextual preferences for web tracking. *Proceedings on Privacy Enhancing Technologies*, 2016(2):135–154, 2016.

[29] G. Merzdovnik, M. Huber, D. Buhov, N. Nikiforakis, S. Neuner, M. Schmiedecker, and E. Weippl. Block me if you can: A large-scale study of tracker-blocking tools. In *2017 IEEE European Symposium on Security and Privacy (EuroS P)*, pages 319–333, NJ, USA, April 2017. IEEE.

[30] Mozilla. Mozilla. `https://support.mozilla.org/en-US/kb/tracking-protection-pbm`, 2017.

[31] A. Narayanan and D. Reisman. The princeton web transparency and accountability project. In *Transparent Data Mining for Big and Small Data*, pages 45–67. Springer, 2017.

[32] PageFair. The state of the blocked web. `https://pagefair.com/downloads/2017/01/PageFair-2017-Adblock-Report.pdf`, 2017.

[33] A. Plus. Adblock plus. `https://adblockplus.org`, 2017.

[34] PrivacyBadger. Privacybadger. `https://www.eff.org/privacybadger`, 2017.

[35] E. Rader. Awareness of behavioral tracking and information privacy concern in facebook and google. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 51–67, Menlo Park, CA, 2014. USENIX Association.

[36] F. Roesner, T. Kohno, and D. Wetherall. Detecting and defending against third-party tracking on the web. In *Presented as part of the 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12)*, pages 155–168, San Jose, CA, 2012. USENIX.

[37] F. Schaub, A. Marella, P. Kalvani, B. Ur, C. Pan, E. Forney, and L. F. Cranor. Watching them watching me: Browser extensions' impact on user privacy awareness and concern. In *NDSS Workshop on Usable Security*, 2016.

[38] I. Seidman. *Interviewing as qualitative research: A guide for researchers in education and the social sciences*. Teachers college press, 2013.

[39] F. Shih, I. Liccardi, and D. Weitzner. Privacy tipping points in smartphones privacy preferences. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 807–816, New York, NY, USA, 2015. ACM.

[40] F. Shirazi and M. Volkamer. What deters jane from preventing identification and tracking on the web? In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, WPES '14, pages 107–116, New York, NY, USA, 2014. ACM.

[41] R. Singel. Online tracking firm settles suit over undeletable cookies. `https://www.wired.com/2010/12/zombie-cookie-settlement/`, 2010.

[42] A. Soltani, S. Canty, Q. Mayo, L. Thomas, and C. J. Hoofnagle. Flash cookies and privacy. In *AAAI spring symposium: intelligent information privacy management*, volume 2010, pages 158–163, 2010.

[43] S. Sudman, N. M. Bradburn, and N. Schwarz. *Thinking about answers: The application of cognitive processes to survey methodology.* Jossey-Bass, 1996.

[44] uBlock. ublock. `https://www.ublock.org/`, 2017.

[45] uBlock Origin. ublock origin. `https://github.com/gorhill/uBlock/`, 2017.

[46] B. Ur, P. G. Leon, L. F. Cranor, R. Shay, and Y. Wang. Smart, useful, scary, creepy: Perceptions of

online behavioral advertising. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 4:1–4:15, New York, NY, USA, 2012. ACM.

[47] R. J. Walls, E. D. Kilmer, N. Lageman, and P. D. McDaniel. Measuring the impact and perception of acceptable advertisements. In *Proceedings of the 2015 Internet Measurement Conference*, IMC '15, pages 107–120, New York, NY, USA, 2015. ACM.

[48] R. Wash, E. Rader, and C. Fennell. Can people self-report security accurately?: Agreement between self-report and behavioral measures. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, pages 2228–2232, New York, NY, USA, 2017. ACM.

[49] Y. Yao, D. Lo Re, and Y. Wang. Folk models of online behavioral advertising. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, CSCW '17, pages 1957–1969, New York, NY, USA, 2017. ACM.

APPENDIX

A. SURVEY ONE

1. How many hours on average do you spend using the Internet each day?
   (a) Less than 1 hour
   (b) 1 - 3 hours
   (c) 4 - 6 hours
   (d) 7 - 9 hours
   (e) More than 9 hours
2. How many Internet connected devices do you own or have access to?
3. Please check all the types of Internet connected devices you own or have access to.
   (a) Personal computers (e.g., desktops, laptops)
   (b) Mobile devices (e.g., smartphones, tablets)
   (c) Activity trackers (e.g., Fitbit)
   (d) "Smart" home-appliances (e.g., Internet connected TV, Refrigerator)
   (e) Other - Write In (Required)
   (f) None of the above
4. Which of the following statements best describe the device you are using to complete this survey.
   (a) Regularly used only by me
   (b) Regularly used by multiple workers at a place of employment
   (c) Regularly used by multiple members of a family
   (d) Regularly used by multiple members who are not members of one family
   (e) Regularly used by many people in a public place (library, Internet cafe, etc.)
   (f) Other - Write In (Required)
5. Do you generally use this device to complete HITs on Mechanical Turk? [Yes / No]
6. Have you heard of the term "Internet/Web tracking"? [Yes / No]
7. (If Yes) In your own words, please describe what "Internet/Web tracking" means to you.
8. (If Yes) In your own words, please describe what comes to your mind when you hear the term "Internet/Web tracking".
9. Please check all the entities that you think collect your information as you browse the Internet.
   (a) The Website you are visiting
   (b) Advertisers and sponsors
   (c) Third-party companies
   (d) Government agencies
   (e) Internet Service Providers
   (f) Browser creators (e.g., Google, Mozilla)
   (g) Other - Write In (Required)
10. In your own words, please list the information you think the entities you checked above collect as you browse the Internet.
11. In your own words, please describe the purposes for which you think the information you listed above is collected.
12. In general, how do you feel about your information being collected as you browse the Internet.
    (a) Extremely Uncomfortable
    (b) Somewhat Uncomfortable
    (c) Not Sure
    (d) Somewhat Comfortable
    (e) Extremely Comfortable
13. In your own words, please explain the reason behind your answer to the above question.
14. Have you taken any steps to prevent your information from being collected as you browse the Internet? [Yes / No / I don't remember]
15. (If Yes) In your own words, please describe the steps you have taken to prevent your information from being collected as you browse the Internet.
16. (If Yes) How confident are you that the steps you describe above prevent your information from being collected?
    (a) Not at all Confident
    (b) Slightly Confident
    (c) Somewhat Confident
    (d) Very Confident
    (e) Extremely Confident
17. Do you use any of the following browser extensions on your current browser?
    (a) AdBlock
    (b) AdBlock Plus
    (c) Ghostery
    (d) PrivacyBadger
    (e) uBlock
    (f) uBlock Origin
    (g) Disconnect
    (h) None of the above
18. For each selected extension (E):

(a) Who installed each of the following browser extensions on your current browser? (Grid)
   i. I installed it myself
   ii. Someone else installed it for me
   iii. I don't remember

(b) How did you learn about extension E?
   i. Friends
   ii. Family
   iii. Social Media
   iv. News
   v. Extension's Website
   vi. Internet Articles
   vii. Other - Write In (Required)
   viii. I don't remember

(c) For how long have you been using each of the following browser extensions? (Grid)
   i. A few days
   ii. A few weeks
   iii. A few months
   iv. A few years
   v. Many years
   vi. I don't remember

(d) Please check all the statements that best describe where you use extension E:
   i. I also use E on a different browser(s) on this device
   ii. I also use E on another device
   iii. Other - Write In (Required)
   iv. None of the above

(e) In your own words, please describe why you use E.

(f) In your own words, please describe how you think E works.

(g) Please state how much each of the following statements indicate your reasons for using E (Strongly Disagree - Strongly Agree):
   i. I use extension E in order to block unwanted content.
   ii. I use extension E because I do not like seeing advertisements.
   iii. I use extension E in order to speed-up the loading of websites.
   iv. I use extension E to prevent websites from serving viruses through advertisements.
   v. I use extension E because I am concerned websites that I visit collect, share or sell my information to other companies.
   vi. I use extension E to prevent online advertising companies from delivering advertisements that are tailored specifically to me.

19. What is your age?

20. What is your annual household income?
   (a) Less than $25,000
   (b) $25,000 to $34,999
   (c) $35,000 to $49,999
   (d) $50,000 to $74,999
   (e) $75,000 to $99,999
   (f) $100,000 to $124,999
   (g) $125,000 to $149,999
   (h) $150,000 or more
   (i) Prefer not to answer

21. What is the highest education level you have completed?
   (a) No High School
   (b) High School Graduate
   (c) Some College
   (d) Bachelor's Degree
   (e) Associate's Degree
   (f) Master's Degree
   (g) Doctoral Degree
   (h) Professional Degree (e.g., MBA, J.D.)
   (i) Prefer not to answer

22. What gender do you most closely identify with?
   (a) Male
   (b) Female
   (c) Other
   (d) Prefer not to answer

B. SURVEY TWO

1. Certain websites "break" or fail to function correctly because of web browser extensions and add-ons such as Ad blockers and Tracker blockers. In the past, has any website(s) failed to function correctly for you as a result of your AdBlocker or Tracker blocker? [Yes / No / I don't remember]

2. (If Yes) In your own words, please describe what functionality or feature of the website(s) failed to function correctly, and list the website(s) on which you experienced this problem.

3. (If Yes) In any given week, how often do you come across websites that fail to function correctly as a result of your AdBlocker or Tracker blocker?
   (a) Never
   (b) Rarely
   (c) Sometimes
   (d) Often
   (e) Always

4. (If Yes) Which of the following best describe the actions you take after you experience a website that fails to function correctly as a result of your Ad blocker or Tracker blocker?
   (a) I ignore the website
   (b) I sometimes attempt to fix the website
   (c) I always attempt to fix the website

5. (If Yes) In your own words, please describe the reason behind your answer to the above question.

6. (If "I sometimes attempt to fix the website" or "I always attempt to fix the website") In your own words, please describe the steps you take to fix the website(s) that fail to function correctly as a result of your Ad blocker or Tracker blocker.

7. (If "I sometimes attempt to fix the website" or "I always attempt to fix the website") In your own words, please describe why you take the steps you describe above.

1. Certain websites detect whether users are running Ad blockers and present them with a message requesting them to disable the Ad blockers in order to continue using the website. In the past, have you come across such messages? [Yes / No / I don't remember]
2. (If Yes) In your own words, please describe the message(s) you observed and list the website(s) you observed these messages on.
3. (If Yes) In any given week, how often do you see messages requesting you to disable your Ad blocker?
    (a) Never
    (b) Rarely
    (c) Sometimes
    (d) Often
    (e) Always
4. (If Yes) Which of the following best describe the action you take after seeing one of these Ad-blocking messages?
    (a) I never proceed to access the content on such websites
    (b) I sometimes proceed to access the content on such websites
    (c) I always proceed to access the content on such websites
5. (If Yes) In your own words, please describe the reason behind your answer to the above question.
6. (If "I sometimes proceed to access the content on such websites" or "I always proceed to access the content on such websites") In your own words, please describe all the steps you take to access the content on websites that ask you to disable your Ad blocker.
7. In your own words, please describe why you take the steps you describe above.