TTPCookie: Flexible Third-Party Cookie Management for Increasing Online Privacy

Ashar Javed, Christian Merz and Joerg Schwenk

Chair for Network and Data Security
Ruhr-University Bochum, Germany
{ashar.javed, christian.merz, joerg.schwenk}@rub.de

Abstract—This paper deals with the problem of privacy issues caused by the tracking activities of web advertisers. Web advertisers place cookies in the browser to track users’ surfing behaviour across websites, mostly without his knowledge or consent. This paper proposes a fine-grained, per-site cookie management protocol. We implement our proposal as Mozilla Firefox add-on and call it TTPCookie. We evaluate the add-on on a data-set obtained from automated visits of 5000 websites. Further, Mozilla Firefox add-ons and other related proposals dealing with cookies and privacy are analysed and compared.

I. INTRODUCTION

Today, web advertisers, who want to track users’ online behaviour, mostly rely on HTTP cookies. With third-party cookies, ad networks link different online sessions of the user and create profiles for targeted advertisement [1]. Ad networks track user’s activities often without their consent or knowledge and it is considered a user’s privacy violation [2], [3], [4]. Web browsers provide limited functionality for the management of third-party cookies. The functionalities include accept all, block all, allow for session and ask user every time for incoming cookies. The available functionality is either user-centric or advertiser-centric.

It is challenging to design third-party cookie management scheme that balance traceability and user privacy. In this paper, we address this challenge and present a fine-grained, per-site cookie management protocol in form of a Mozilla Firefox add-on (see Section III). Our proposal enables behavioral targeting with low privacy risks.

Our add-on provides an improved management of third-party cookies, enforcing fine-grained, per-site cookie management. It builds editable lists (whitelist, blacklist and trusted third-party list) of advertisers. The add-on also counts third-party cookie usage and can limit the use of a cookie when a given threshold is reached. Also, instead of a count threshold, the add-on can start blocking after a prescribed amount of time. Finally, users can also check the number of first-parties sharing the same third-party cookie.

It is reasonable to expect privacy-conscious users to make a limited number of high-level privacy decisions and builds lists of advertisers. However, for most users, entering the lists of advertisers is difficult as it requires an understanding of a given domain name. In order to help these users, the add-on also offers the option to download predefined configuration lists. We rely on Privacychoice (http://privacychoice.org/) in order to develop third-party advertiser lists (whitelist, blacklist and trusted third-party list) (see Section IV-G).

In this paper, we also present a study on the deployment of third-party cookies in web applications (see Section IV). For this purpose, we collected a data-set of top 5000 websites according to Alexa index [5]. We found 49,054 third-party requests during automated visit of 5000 websites. It shows an average of 10 third-party requests per first-party domain. In the survey, we also give evidence of other tracking techniques such as local shared objects and DOM storage (see Section IV-E). Given the widespread use of third-party cookies, for now we limit the further discussion to third-party cookies. Our results also show that the footprint of third-party cookies is a legitimate cause for privacy concern [6].

We also evaluate TTPCookie on the data-set of top 5000 websites (see Section IV-F). Our results show that the add-on does not block HTTP requests, but only removes selected cookies from requests if they violate user-defined policies. We found 49,054 third-party requests during the automated visit of 5000 websites. Of those 83.29% (40,857) were modified by add-on (at least one third-party cookie was blocked) because of given policies.

A. Cookies

Web applications use HTTP Cookies to maintain session states between client and server. Cookies consist of key-value pairs stored in the browser and sent with every request.
to the server. A website is called first-party domain if the user is accessing the contents of the web application directly (i.e., directly visited domain or whose web address in the browser’s address bar) and the cookie associated with this is called first-party cookie. Web pages often contain additional elements like images, scripts, stylesheets and Flash objects etc. For fetching these elements the browser performs additional HTTP requests. Some of the requests may address different domains (i.e., the domain other than the one in the address bar) and we call these domains third-party domains. The cookies associated with third-party domains are called third-party cookies.

B. Online Advertising

The online advertising world is complex with parties playing different roles. We give a brief overview of the terminology [14]:

- **Advertiser:** “a party with online ads that wants to embed ads in web pages. The advertiser is willing to pay for this service”.
- **Publisher:** “a party with a web page (or web site) and willing to place ads from others on its pages. The publisher expects to be paid for this service”.
- **Ad network:** “a party who collects ads (and payment) from advertisers and places them on publisher’s pages (along with paying the publisher). Example ad-networks include Google, Yahoo and MSN”.
- **Behavioural Tracking:** “refers to the use of users’ information about previously and currently browsed web pages across the web”.

C. Contributions

This paper makes the following contributions:

- We give users a system for fine-grained, per-site third-party cookie management in the form of Mozilla Firefox add-on.
- This paper presents a study on the usage of third-party cookies in 5000 websites and also show the impact of our add-on.
- We compare the functionality of our proposal with other privacy-preserving add-ons and proposals.

II. BACKGROUND

We have used an experimental add-on named privaCookie [7], [8], as a base for the development of our proposal. Instead of completely blocking third-parties’ cookies, the user can choose privaCookie’s global configuration regarding how much private information he is willing to reveal. Options for setting the amount of third-party cookie usage are given by numeric values for their “maximum sendings” and their “maximum age”. A blocked cookie is usually reset by the third-party with a new value. This enables the user to control amount of tracking done by advertisers.

Now, we give a short overview of privaCookie functionality. The add-on privaCookie monitors incoming and outgoing HTTP traffic for third-party requests. The domain name opened in browser’s tab is referred as first-party and all communication from this tab with another domain is classified as third-party. This way of identifying third-party requests works in a reliable manner and does not depend on the initialising resources (scripts, frames and images etc).

In privaCookie, each third-party request is examined for cookies. Incoming cookies are stored and outgoing cookies are compared to a list of already known cookies. By storing the first-party along with its cookie contents, privaCookie ensures that no third-party will get the same cookie key-value pair from different first-parties. Add-on privaCookie additionally checks the HTTP referrer and shortens it to remove possible tracking or identification strings.

**Threat Model:**

The adversary model that we consider through the rest of the paper is same as described in privaCookie. According to privaCookie [7]:

“Users’ privacy with respect to online advertisers and malicious adversary is protected if the users have the ability to prevent third-parties from tracking their activities online and have some sort of control over cross-site requests. We do not consider a case where “whitelisted” advertisers start selling the users profiles to other ad networks”.

III. FLEXIBLE THIRD-PARTY COOKIE MANAGEMENT

Our solution is capable of enforcing third-party cookie policies on a per-site basis depending on user’s preferences in “editable lists”. The solution is automated and allows users to control the amount of information they are willing to share.

A. Third-party Lists Editor

We present a third-party list editor to the user (see Figure 1). The decision to use the third-party cookie across different websites depends on lists (whitelist, blacklist and trusted third-party list). The user can use the arrow buttons to move entries in respective lists. The third-party editor dialog also provides an option to download predefined lists of advertisers. The downloaded entries are merged into the existing third-party lists. In order to develop, predefined lists, we have used Privacychoice (http://privacychoice.org/).

We refer to section IV-C for more details.
• **Whitelist:** The advertisers in this list get the third-party cookie unmodified.
• **Blacklist:** The advertisers in this list never get the third-party cookie.
• **Trusted Third-party List:** The advertisers in this list get the third-party cookie but according to the user’s settings.

![Figure 1. Third-Party Editor with three lists.](image)

**B. Fine-grained Settings Dialog**

We also present settings dialog to the user so that the users can control the amount of tracking (see Figure. 2). More specifically, the following fine-grained policy management options are available:

• **Temporal Tracking:** In order to provide temporal tracking policy, the same cookie to the same third-party advertiser is used only for a limited number of times, when a user visits a specific website.
• **Spatial Tracking:** In order to provide spatial tracking policy, that is, to protect user’s privacy when a user visits multiple sites that need to send cookies to the same third-party advertiser, new cookies will always be sent if the third-party advertiser is not in the whitelist and if policy permits.

**C. Improvements over privaCookie**

In this section, we discuss the improvements that we made over an experimental add-on privaCookie.

1) **User Interface:** One of the goal of add-on is to give the user a supportive user-interface[2]. A user can add a toolbar button (see Figure. 3). It is the main controlling element and provides activating/deactivating options along with “state” indicators, “action” indicators and “context menu” option in the form of drop-down arrow. The add-on’s state indicator is either “active (green color)” or “inactive (red color)”. The “action” indicators start blinking when a certain action takes place. The “action” indicators are:

• **W:** means whitelist third-party detected and that party can receive the cookie.
• **B:** means cookie has been blocked because the advertiser is part of user’s blacklist. By default, whenever a new third-party detected, we added advertiser to the blacklist.
• **TP:** means trusted third-party list and the cookie has been sent if user-defined policy permits.
• **#:** When # sign starts blinking, it means that a cookie has been used too many times or is too old to be resent and therefore blocked.

The “context menu” provides options like “help”, “verbose mode”, “show whitelist”, “show blacklist”, “edit third-party list”, “settings dialog” and “about”.

2) **Cookie Storage:** In privaCookie, cookie storage is not persistent and each restart of the add-on requires a deletion of all available cookies to ensure its functionality. This will also delete cookies required by the user, e.g., login cookies or shopping baskets. Our add-on stores cookies persistently in a database. The add-on creates `add-onnamehere.sqlite` in the user’s profile directory to save cookie information. One of the challenges we have faced is performance issue because of continuous querying the database during normal browsing. We overcame this
challenge with the help of a cache layer which loads all entries once from the database and stores in memory for further operations. All changes are written back to the database on browser close.

3) Privacy/Traceability Trade-off: The add-on privaCookie manages all third-party cookies in a privacy-preserving manner. According to privaCookie:

“Our solution enables advertising to have differentiation capabilities without allowing for excessive tracking of users online.”

The privacy/traceability trade-off as depicted in privaCookie can be seen in Figure 4. At position (1,0), the third-party cookies management policy allows for the complete tracking of users online and at position (0,1), blocking all third-party cookies impedes online tracking by third parties. In our proposal, we have extended this trade-off by adding whitelist and blacklist functionality (see Figure 5).

4) Spatial and Temporal Tracking Policy: For consistency, we have chosen the same notation as described in privaCookie. It defines the set of first-parties as $B$ with elements $b_i$, while the different indices represent distinct domains. Third-parties are similarly described with $D$ and $d_j$. Cookies are contained in set $C$ and identified by $c_{i,j}$ with the first index representing the first-party domain and the second index representing the third-party domain. Cookies and domain names are available in the browser history set i.e., $H$. There are two tracking policies defined in privaCookie:

**Spatial Tracking Policy:** In order to protect user’s privacy when a user visits multiple first-party domains that need to send cookies to the same third-party advertiser, new cookies will always be sent. The implementation of privaCookie only supports the hard coded value of $L_S$ i.e., $L_S = 1$ where $L_S$ is a spatial tracking limit/threshold.

$$\sum_{b_m \in H(B)} \beta(b_m, d_j, c_k) < L_S$$

In case of our proposal, the value of $L_S$ depends upon user. User can choose the number of first-parties sharing the same third-party cookie.

**Temporal Tracking Policy:** When a user visits a specific website, the same cookie to the same third-party advertiser is used only for a specified time period $L_T$ or for a limited number of site’s visits $L_V$.

$$\sum_{b_m \in H(B)} v(b_m, d_j, c_k) < L_V$$

The above definition can be written in same form for $L_T$. In our add-on, we have implemented this policy in the same spirit as given in privaCookie.

IV. SURVEY

In this section, in order to investigate the use of third-party cookies for tracking, we present the results of our survey of Alexa’s 5000 websites. In the next sections, we discuss the worth mentioning aspects of our survey.

---

3 The detailed information about the survey is available at [http://www.chm-software.com/ttpCookie/?p=overview](http://www.chm-software.com/ttpCookie/?p=overview)
A. Data Collection

In this section, we briefly discuss our data collection methodology. We have used the FourthParty tool \[9\] to collect the HTTP requests' data of Alexa's 5000 websites. To automatically visit websites, we have also implemented a small add-on whose job is to call the list of domains from a text file. During the data collection process, our add-on is active in the currently running instance of Mozilla Firefox browser. The sample fine-grained policy that we have set in the setting dialog (see Section [III-B]) at the time of data collection is:

- Maximum age of the third-party cookie is set to two (2) minutes,
- Maximum transmissions of third-party cookies is three (3) times,
- Maximum number of first-parties sharing the same third-party cookie is set to two (2).

With our infrastructure we automatically visited the websites in a time frame of about 10 hours. All collected data is retained from the temporary profile directory and transferred into SQL database tables to facilitate further analysis.

B. Identifying Third-Parties

We have first checked the SQL database for the count of distinct third-parties. This leads to a list of 1200 domains, taken from the statistics log of add-on. We have also compared this result to domains’ information stored in the internal Firefox cookie table. During comparison, we have ignored already known 5000 first-parties. As a result, we found 909 distinct domains acting as third-party only. This turns out that approximately 25% of third-parties are also acting in the role of a first-party and that’s why they belong to the list of 5,000 visited domains.

C. Inspecting Third-Parties

We ordered our list of identified third-parties by their absolute usage count in distinct first-party websites (see Table [I]). The number of total requests sent to a third-party does not match its position in the usage ranking in each case. Some first-parties make heavy use of a certain third-party which causes a significant rise in the request count.

We found out that all identified third-parties are used from 20 – 1130 distinct first-parties (see Figure [http://i.imgur.com/tvV1a7.jpg]). The list leader is doubleclick.net which covers ≈ 23% of our website visits. During automated visits of 5,000 websites, we recorded a total number of 49,054 third-party requests – an average count of 10 (= [49,054/5,000]) requests per first-party domain.

D. Looking at First-Parties

For each first-party, we analysed its usage of distinct third-parties (see Table [II]). 1967 first-parties (39.34%) did not use any third-party content while 3033 first-parties (60.66%) connected to one or more distinct third-party hosts. The website knowyourmeme.com came out as the heaviest user of third-parties with 57 requests to distinct third-party domains. The complete overview (see Figure [http://i.imgur.com/8vXi00y.jpg]) shows that the majority of visited websites make use of third-parties and approximately 50% of them utilise more than one third-party domain.

291 first-parties (5.82%) are acting as third-parties for other visited first-party domains and therefore categorised as “hybrid-parties”. These are hard to identify for a user as they cannot be detected by simply watching the cookies stored in Firefox browser. A general blocking of cookies for “hybrid-parties” would stop their third-party activities but it can affect browsing experience when visiting as first-party. We have also found out that 1256 visited domains (25.12%) did not set any first-party cookies. This does not imply that there are no third-party cookies set by these websites. During analysis, we counted the domains which have no first-party cookies but indirectly created cookies by including third-party content. This leads to 244 first-parties (4.88% of 5,000 visited domains; 19.43% of 1,256 first-parties without immediate cookies).

E. DOM Storage, Local Shared Objects and Cookies

After 5000 websites automated visits, Firefox contained a total number of 20654 cookies from 4560 different domains in its internal storage. We also found 392 elements in

### Table I

<table>
<thead>
<tr>
<th>Pos.</th>
<th>TP-Domain</th>
<th># FP</th>
<th>% FP</th>
<th># Requests</th>
<th>% Requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>doubleclick.net</td>
<td>1150</td>
<td>22.60</td>
<td>5240</td>
<td>10.68</td>
</tr>
<tr>
<td>2.</td>
<td>facebook.com</td>
<td>977</td>
<td>19.54</td>
<td>3160</td>
<td>6.44</td>
</tr>
<tr>
<td>3.</td>
<td>google.com</td>
<td>970</td>
<td>19.40</td>
<td>3365</td>
<td>6.86</td>
</tr>
<tr>
<td>4.</td>
<td>scorecardresearch.com</td>
<td>579</td>
<td>11.58</td>
<td>1762</td>
<td>3.59</td>
</tr>
<tr>
<td>5.</td>
<td>twitter.com</td>
<td>512</td>
<td>10.24</td>
<td>1788</td>
<td>3.64</td>
</tr>
<tr>
<td>6.</td>
<td>quantserve.com</td>
<td>391</td>
<td>7.82</td>
<td>924</td>
<td>1.88</td>
</tr>
<tr>
<td>7.</td>
<td>imrworldwide.com</td>
<td>210</td>
<td>4.20</td>
<td>282</td>
<td>0.57</td>
</tr>
<tr>
<td>8.</td>
<td>adxns.com</td>
<td>180</td>
<td>3.60</td>
<td>520</td>
<td>1.06</td>
</tr>
<tr>
<td>9.</td>
<td>yieldmanager.com</td>
<td>179</td>
<td>3.58</td>
<td>475</td>
<td>0.97</td>
</tr>
<tr>
<td>10.</td>
<td>2o7.net</td>
<td>163</td>
<td>3.26</td>
<td>246</td>
<td>0.50</td>
</tr>
<tr>
<td>11.</td>
<td>yadro.ru</td>
<td>146</td>
<td>2.92</td>
<td>319</td>
<td>0.63</td>
</tr>
<tr>
<td>12.</td>
<td>baidu.com</td>
<td>144</td>
<td>2.88</td>
<td>1017</td>
<td>2.07</td>
</tr>
<tr>
<td>13.</td>
<td>revsci.net</td>
<td>139</td>
<td>2.78</td>
<td>350</td>
<td>0.71</td>
</tr>
<tr>
<td>14.</td>
<td>serving-sys.com</td>
<td>139</td>
<td>2.78</td>
<td>311</td>
<td>0.63</td>
</tr>
<tr>
<td>15.</td>
<td>addthis.com</td>
<td>131</td>
<td>2.62</td>
<td>546</td>
<td>1.11</td>
</tr>
<tr>
<td>16.</td>
<td>yandex.ru</td>
<td>128</td>
<td>2.56</td>
<td>374</td>
<td>0.76</td>
</tr>
<tr>
<td>17.</td>
<td>gemius.pl</td>
<td>127</td>
<td>2.54</td>
<td>412</td>
<td>0.84</td>
</tr>
<tr>
<td>18.</td>
<td>atdmt.com</td>
<td>116</td>
<td>2.32</td>
<td>245</td>
<td>0.49</td>
</tr>
<tr>
<td>19.</td>
<td>ivwbox.de</td>
<td>113</td>
<td>2.26</td>
<td>259</td>
<td>0.52</td>
</tr>
<tr>
<td>20.</td>
<td>criteo.com</td>
<td>111</td>
<td>2.22</td>
<td>229</td>
<td>0.46</td>
</tr>
</tbody>
</table>

**Table I**

TOP 20 THIRD-PARTIES ORDERED BY NUMBER OF DISTINCT FIRST-PARTY HOSTS
<table>
<thead>
<tr>
<th>Pos.</th>
<th>Domain</th>
<th># TPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>knowyourmeme.com</td>
<td>57</td>
</tr>
<tr>
<td>2.</td>
<td>hongkiat.com</td>
<td>44</td>
</tr>
<tr>
<td>3.</td>
<td>digitalspy.co.uk</td>
<td>42</td>
</tr>
<tr>
<td>4.</td>
<td>sport1.de</td>
<td>41</td>
</tr>
<tr>
<td>5.</td>
<td>cuantaraazon.com</td>
<td>36</td>
</tr>
<tr>
<td>6.</td>
<td>dailycaller.com</td>
<td>29</td>
</tr>
<tr>
<td>7.</td>
<td>premiereleague.com</td>
<td>29</td>
</tr>
<tr>
<td>8.</td>
<td>thisissouthwales.co.uk</td>
<td>28</td>
</tr>
<tr>
<td>9.</td>
<td>mysearchproperties.com</td>
<td>28</td>
</tr>
<tr>
<td>10.</td>
<td>anime44.com</td>
<td>28</td>
</tr>
<tr>
<td>11.</td>
<td>wetter.com</td>
<td>28</td>
</tr>
<tr>
<td>12.</td>
<td>radaronline.com</td>
<td>27</td>
</tr>
<tr>
<td>13.</td>
<td>bostonherald.com</td>
<td>26</td>
</tr>
<tr>
<td>14.</td>
<td>allkpop.com</td>
<td>25</td>
</tr>
<tr>
<td>15.</td>
<td>gamestar.de</td>
<td>25</td>
</tr>
<tr>
<td>16.</td>
<td>socialmediaexaminer.com</td>
<td>25</td>
</tr>
<tr>
<td>17.</td>
<td>boston.com</td>
<td>25</td>
</tr>
<tr>
<td>18.</td>
<td>mediatakeout.com</td>
<td>24</td>
</tr>
<tr>
<td>19.</td>
<td>freekaamaal.com</td>
<td>23</td>
</tr>
<tr>
<td>20.</td>
<td>breitbart.com</td>
<td>23</td>
</tr>
</tbody>
</table>

Table II
TOP 20 FIRST-PARTIES ORDERED BY NUMBER OF DISTINCT THIRD-PARTY HOSTS

the DOM Storage created by 253 distinct domains and at the same time there were 90 distinct domains which created Local Shared Objects (LSOs). Only a small subset of third-parties are making use of DOM storage and LSO as compared to the use of cookies in wild (see Table III).

<table>
<thead>
<tr>
<th>Type</th>
<th>Count</th>
<th>Domains</th>
<th>thereof Third-Parties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cookie</td>
<td>20.645</td>
<td>4.560</td>
<td>909</td>
</tr>
<tr>
<td>DOM Storage</td>
<td>392</td>
<td>253</td>
<td>11</td>
</tr>
<tr>
<td>LSO</td>
<td>90</td>
<td>90</td>
<td>49</td>
</tr>
</tbody>
</table>

Table III
RELATION BETWEEN COOKIES, DOM STORAGE AND LSOs

F. Evaluation

We evaluate our proposal on a data-set of 5000 websites. First we automatically visited the 5000 websites (taken from Alexa’s index) without add-on installed and collected a total number of 364867 HTTP requests. Next, we visited websites with add-on installed and enabled and this resulted in 359326 HTTP requests. The difference between the measured HTTP requests is 1.52% and therefore negligible. Our results show that our add-on does not block HTTP requests, but only removes selected cookies from requests if they are violating the user-defined policy. We found 49.054 third-party requests during automated visit of 5000 websites and of those 83.29% (40.857) were modified by the add-on (at least one third-party cookie was blocked) because of the given policy violation. We also found out that the third-parties do not initiate further tracking actions if they detect a missing cookie – they simply assign a new value in the following regular connection.

G. Rating Third-Parties

Our add-on’s third-party editor offers the option to download predefined lists (blacklist, whitelist and trusted third-party list). We need a reliable rating of third-parties to create these lists and initially planned to make lists by categorising first-party domains. We also wanted to identify the relations between third-parties and categories to detect their trust level. e.g., a third-party that is only used on adult websites could be an entry in the blacklist for some users.

There exists different online categorisation platforms but they do not provide enough information to finalize the categorisation process. An automated crawl of alexa.com and dmoz.org allowed us to assign categories for 2,877 of the requested 5,000 domains. Both platforms did not offer any categorisation data for the remaining 2,123 domains (42.46%), so we had to search for another method to fill the lists.

The alternative solution, we found, was a direct classification of third-party domains provided by the tracker and advertiser database on privacychoice[20], [21]. Privacychoice offers detailed information for a large number of third-parties, combined with a rating system. Free automated access is not possible and we had to check each domain manually. Therefore, the list of 1200 identified

4 alexa.com, dmoz.org, zvelo.com, ...
third-parties was reduced to 172 entries by choosing only those which are included from minimum 10 different first-party domains.

**Privacychoice**’s rating system assigns classification values between zero and 50 and marks them with supportive colors (see Figure 6). The rating “No PrivacyScore” is the most positive and shows that a third-party is not taking user data for tracking or does not even collect it at all – therefore we place these providers on whitelist. Third-parties rated with “comfort” are moved into trusted third-party list and each other domain (classified as untrusted by "caution", "concern", or unknown state) goes to the blacklist. Table IV shows the results of our rating of 172 third-party domains. We refer to [20], [21] for the detailed description of the rating system.

V. RELATED WORK

In this section, we compare the presented approach with closely related proposals.

A. Ghostery

Ghostery add-on [10] contains a large database of third-party content and shows a notification to the user when third-party content is found in a website. Ghostery does much more than controlling cookies. It can also control scripts, images and other elements but Ghostery works in binary way i.e., the user can allow or disallow third-party contents. Ghostery does not provide fine-grained policy management. At the same time Ghostery depends on a frequently updated database. In our add-on, a user can set the fine-grained cookie policy and it does not depend on frequently updated database. We also give the user more control over his/her private information.

B. BetterPrivacy

BetterPrivacy add-on [11] deals with Local Shared Objects (LSOs) and DOM storage. A user can delete the LSO and DOM storage objects in a selectable time interval or on browser starts. The user gets a notification about new LSOs and can modify them via an integrated editor. In BetterPrivacy, only whitelist option is available to the user and at the same time it does not deal with third-party cookies which is by far the most frequently used tracking method. Our add-on gives better control regarding the commonly used tracking technique and provides fine-grained cookie policy management.

C. Do Not Track

Do Not Track (DNT) [12] is a proposal that enables privacy-concerned users to opt out of tracking done by websites. According to Jonathan R. Mayer [12]:

**Do Not Track** signals a user’s opt-out preference with an HTTP header, a simple technology that is completely compatible with the existing web. Several large third parties already honor Do Not Track, but many more have been recalcitrant. We believe regulation is necessary to verify and enforce compliance with a user’s choice to opt out of tracking.

The main problem with DNT is its reliance on third-parties to honor users’ preference which is not happening in reality [13]. In our solution, the control is in user’s hands and we do not assume any sort of regulation.

D. Adnostic

Another closely related proposal i.e., Adnostic [14] also addresses the problem of online tracking with the help of in-browser system that uses homomorphic encryption and efficient zero-knowledge proofs. Adnostic is constructed to prevent advertisers from learning about the user’s actions. Similar to DNT, the main problem of Adnostic is its reliance on third-parties to honor the users’ settings and we believe, this is not the case today. In our approach, we give control to the user so that he can decide. Our proposal enables tracking with minimal privacy risks.

E. Privad

Privad [15] does not trust ad-networks and anonymizes every piece of information sent by the client. This anonymization impacts on performance and Privad does not attempt to balance the desire of ad networks to track users via third-party cookies and at the same time allows users to control the amount of private information they are willing to share. Our solution is better than Privad in a sense that user can trust on some ad-networks with the help of policy.

F. Collusion

Collusion [17] is an experimental add-on for Firefox and allows users to see the tracking done by third-parties in the form of spider-web. In its current form Collusion does not have opt-out tracking option and will depends on a global database of web trackers. Our proposal allows users to set policies and gives more control over their private information.

G. Extended Cookie Manager

Extended Cookie Manager add-on [16] is now outdated and in its current form is not compatible with Firefox. Also on the Mozilla add-on reviews there are complaints from users that it causes problem even in previous versions of Firefox.

H. Beef Taco – Targeted Advertising Cookie Opt-Out

Beef Taco [18] floods the browser with opt-out cookies and at the same time provides no configurable and easy to use interface. Opt-out cookies are only useful if the ad-networks decide to actually respect them. Our solution gives user more control to define cookie management policy.
I. Doppelganger

Doppelganger [19], a novel system for creating and enforcing fine-grained, privacy preserving cookie policies in web browsers. Doppelganger has the following drawbacks. It has huge performance cost because of Doppelganger’s mirroring mechanism. In Doppelganger, every action of the user is mirrored and every HTTP request in duplicate sent back to the server. It has a long training period and depends on user’s comparison between the main and fork window in order to define the policy. Last but not the least, Doppelganger simply blocks all third-party cookies. In TTPCookie, we give user a functionality to make editable lists (whitelist, blacklist and trusted third-party list) of service providers.

VI. CONCLUSION AND FUTURE WORK

We proposed a fine-grained, per-site cookie management add-on named TTPCookie. We implemented our proposal as Mozilla Firefox add-on. As a part of future work, we plan to do a usability study with users of different age and knowledge in order to see what problems and difficulties users have to face when defining fine-grained third-party cookie policy and how we can solve them. We also plan to make the third-party rating system automatic.

REFERENCES


