User Agent and Privacy Compromise

Jianhui Zhu, Bipin C. Desai

June 25, 2015

Abstract

World Wide Web and the graphic user agents(web browsers) have brought the internet to billions of new users who use it hours on end daily to perform a multitude of tasks. However, the user agents also provide a means to compromise the users privacy by employing various tracking mechanisms and use of analytics. The browser was intended to make the use of the internet easy with a simple and intuitive interface. It has morphed into a beast which has hidden in it mechanisms to allow suppliers of information content, on-line shopping companies and multitude of third parties to target publicity based on information gleaned from previous web journeys of users of these browsers. This paper focuses on summarizing privacy problems on the client side and highlights the default settings of some of the popular browsers and points out the difficulty of creating the proper settings even to disable cookies from third parties. We present some independent add-ons to help in preserving some privacy and some of the drawbacks of such band-aid solutions. Finally, we present some suggestions so that the user can know exactly what is being recorded in the cookies based on double encryption giving back some control to the user of his own data.

Categories and Subject Descriptors K.4.1 [Public Policy Issues] Abuse and crime involving computers, Privacy: K.6.5 [Security and Protection] Invasive software

Keywords: C3S2E, cookies, user agent, compromise privacy, internet pirates

1 Introduction

The first web browser named “World Wide Web” was introduced [29] in 1990; it was renamed Nexus to avoid confusion with the internet application of the same name. Many changes have been made not only in the protocols, namely the hypertext transport protocol (HTTP - the web transport protocol) and the Hyper Text Markup Language (HTML), but also in the browsers. The reason for this was the obvious rush to finish with limited budget at an institute(CERN) not in the business of computing but in nuclear research. Since those exciting days in the mid 1990s, when researchers and businesses flocked eagerly by the hundreds and soon thousands to the early meetings of the WWW one sees the nefarious result of the laissez-fair attitude coupled with the ignorance of the regulating bodies. The businesses, without any public oversight, are influencing the development of the protocols and the browsers. This far reaching influence of business is illustrated by the recent controversial introduction of ’Encrypted Media Extensions (EME)’ in HTML5 by the World Wide Web Consortium (W3C). EME is a new application programming interface (API) to allow non-free web-based music and video services. According to media reports [6] this move was clearly orchestrated by the music and film industries.

As the web and the browsers for it reach a quarter of a century span we see the extent to which it has engulfed all parts of modern life and is impacting on personal privacy and even security of the person and the state. As a software application for retrieving, presenting and traversing information resources on the World Wide Web, web browser use a Uniform Resource Locator(URL) to access contents. At present, web browsers are everywhere and used for a myriad of tasks; both for professional and personal use. For example, users may use a web browser to read news, watch movies or read business reports. Although web browser has streamlined and provided an efficient mechanism for information exchange, the evolution of HTTP and HTML and the pressure of businesses to adapt the browser design, from the very start of the web, to their need rather than that of users leads to a compromise of user’s privacy and security. For example, users browsing history maybe be used by third parties; users may receive targeted publicity and malicious JavaScript code; users may unwittingly install malicious browser extensions which steal their input, redirect URL access spam, Online Social Network (OSN) messages and unsolicited publicities. According to the recent report prepared by the Office of the Privacy Commissioner of Canada [21] and summarized in [33], a non-significant number of personal and sensitive advertisements(ads) presented to the users were based on searches. More of the same is occurring when free email offering sites scan the emails of people who use these popular 'free' services.

This paper focuses on categorizing the cause of current web-browser problems, briefly discuss how specific web browsers, protocols and user preferences could easily be exploited by not only the established suppliers of contents but directly and indirectly by third parties to achieve their own objectives; this can range from commercial advantage to malicious intent. In this paper we pinpoint the weaknesses of the protocols, privacy related browser issues and the lack of finer control offered by the popular browsers and suggest some band-aid work around solutions. We will attempt to explain how these solutions work, the advantage and disadvantage of these solutions and suggest possible new solutions.

While current research on browser security mainly focuses on specific topics [19], this paper gives the ordinary users some guidelines to enhance their privacy and suggestions for future work to enhance privacy features by suggesting security measures in web browsers. One of the extreme solutions would be to device a new web, which would be non-commercial and likely paid directly by the users using a transfer protocol limited between the supplier and the consumer and his reworked user agent which would include features to parse the source content sent both by servers and clients and include the features needed to prevent privacy violation and malicious bugs.

In the next sections we discuss the following topics: the need for cookies and accepting third party content; what is typically stored cookies; third party cookies; how cookies are used to track users without their consent knowledge or notification of cookies being stored. A discussion about effectiveness of add-ons such and the futility of setting non-enforced features such as “Do Not Track”. This is a voluntary feature not enforceable and falls in the category of stopping robocalls and the “Do Not Call Registry” which has been reported to be entirely counterproductive. [13].

2 Privacy Related Elements

2.1 HTTP Protocol

The hyper text transport protocol(HTTP) was designed to provide information, essentially from a server to a client. Users were expected to use a user agent (now commonly refereed to as web browsers or simply browsers) to communicate with the HTTP server. The definition of the initial protocol used at CERN was actually re-written a few years after the initial introduction of the web [29].

As noted in the initial specification of the HTTP/1.1 protocol [30], it was recognized the there are issues of privacy and need for security not only in the browser but also in the http server. The browser is the channel through which sensitive personal information is transmitted and often stored locally; some of which is transmitted to the server as well and used for authentication and validation. This information include: names, user IDs, secret keys and passwords, account numbers, address, email address, DOB. The browser must not allow compromise of any of this information. The designer of the HTTP protocol had recommended the need for convenient interface for the user to control what information is kept and how to use it.

The HTTP server is privy to some of the above personal information including the user's IP address and the URL of the request. A series of requests from the user could be recorded by the server to determine the users interests and exploit it for commercial and/or unsavoury purposes. This is what is actually happening with today's search engines(SE) and online social networks(OSN). Some of the algorithms in OSN are designed to get a profile of the users from their interaction to such an extent that the OSN knows users better than their close friends [5]!

Finger printing an user through IP address can be avoided as the user moves around from coffee shop to coffee shop or is assigned a new dynamic IP address by the ISP or by use of onion routing for anonymization. However things such as starting address can be gleaned from repeated requests such as driving directions which usually starts from the user's home. Cookies, on the other hand, can serve as an identifier regardless of the change in IP address [9].

2.1.1 Cookies

HTTP is memoryless (also called stateless and being idempotent in the original document [29]) and the web server was originally meant not to maintain the user's browsing history. This was done so as to avoid storing this information from a multitude of users of an HTTP server, many of whom may never return. Also, permanent storage was not quite as cheap a few decades ago! The protocol was called idempotent since the same request using a given URL would result in the same web content from the server (provided the content had not been modified). Cookies contain server specified arbitrary information and were introduced to maintain the record of an users recent (past) browsing activity at the server; thus a cookie stores the state relevant information and stored on the users hard disks [15]. The server gets a free ride thanks to the privacy ignorance of the protocol [27], [25], [28] exploiting the software features 'dictated' by interested commercial organizations to be built into the browsers. For example, a browser is required to be able to store a minimum number of cookies for each domain and each cookie is required to be at least of a given minimum size.

Cookies contains information such as: the user identifier, a database key and additional information which the server may need to verify the user's future requests and to record the recent log of the user's requests which could be used to tailor the contents of the subsequent pages sent from the server. At the same time, this history can also be used to track the user's visits. While cookies are stored locally, the browser is required to allow access of the cookie to the server that had set it [4].

2.1.2 Cookies type

Cookies can be classified into two groups: first-party cookies and third-party cookies; there are no second party cookies! According to the IETF/RFCs, a cookie, is a small amount of data that the server sends to the client to be stored in the clients stable storage. The information is in the form of an attribute/value pair format and is valid for a set of URLs. Any future request from the client which refers to an URL in the set would include the data from the relevant cookie. In this way the server can determine the history of previous transactions with the client. If first-party cookies were disabled, a Web site could not be able to keep track of the client's past activity nor could it identify the client as the one seen before and hence make any on-going interaction possible. For example, applications such as shopping could not be possible [10]. Also, some sites would refuse to serve contents if cookies for the site are not allowed.

The third party cookie is similar to the first party cookie but is for a domain name other than the one the user is currently visiting. By default, third-party cookies are allowed by many web browsers; however, they may be blocked, as they are widely used by advertisers to track browsing history [26].

In general, web server applications set-cookies on client computers to identify the user(username, password); additional information in the cookie varies with the web application. For example, shopping web application may save user's virtual shopping cart at least partially at the client site and optionally other information at the server site. The following is an example which represents a typical use of the information stored in a cookie.

As given in the Term and Condition(e.g., [17]) of a typical search engine, the operator would track users' preferences (language, region), users' search keywords used in their searches, their interaction with the advertisement owner when a user clicks the paid listing on the search result pages. In addition, it also records user‘s action to a content provided by the search engine. For example, a video streaming site would record user's latest watched video information saved as “recently_watched_video_id_list” cookie.

2.1.3 Storing Cookies

According to HTTP State Management Mechanism [27], [28], a server saves cookies on client internet devices by sending “set-cookies” header, with predefined-format attributes(value, expires-date, domain, path and secure).

Cookies could also be set and got by using JavaScript embedded in the web content sent by a server as shown in codes given below.

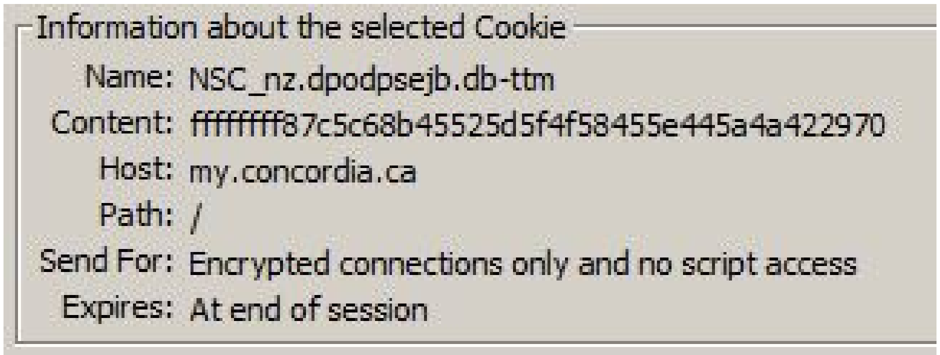
```
function setCookie(c_name,value,expiredays)
{
  var  exdate=new Date();
  exdate.setDate(exdate.getDate()+expiredays);
  document.cookie=c_name+ ”=” +escape(value)+
  ((expiredays==null)? ”” :”; expires=”+exdate.toGMTString());
  }

function getCookie(c_name)
{
  if(document.cookie.length>0)
    {
      c_start= document.cookie.indexOf(c_name + ”=”);
      if(c_start!=-1)
      {
        c_start=c_start + c_name.length+1;
        c_end=document.cookie.indexOf(”;”,c_start);
        if(c_end==-1)
        c_end=document.cookie.length;
        return unescape(document.cookie.substring(c_start,c_end));
        }
      }
      return ””;
}
```

As shown in the code above, cookies are easy to set and also easy to get from users internet devices. Although cookies are widely used by web application/service providers to track users interaction during their browsing activities, only a small percent of users are aware of or if attempt to protect their privacy. Since the cookies are encrypted, even the user cannot determine its contents. Many browsers do not have a good facility to examine even the basic contents of the cookies. According to a recent study [24], although 77% of web users are concerned about web security, only a small fraction of them (around 13%) fully understand how cookies work. Moreover, 62% survey respondents consider that knowing the purpose of an internet cookies is vital and 56% think it is very important to know how to delete cookies. In spite of this, around 18% of the users accept all cookies and 37% people have no idea how they can manage their cookies on their own devices.

Some web applications may inform users about the agreement of using cookies, others may not. So actually users̀ personal information would be tracked without them being aware of it! This is really problematic for third-party cookies.

The third party cookies are set when users access a domain server which provides contents included in which is third party contents. For example, a user accesses a page from www.A.com/pageA; this web page could include contents from. for example a third party such as: www.B.com; this is done using a mechanism such as: src=www.B.com/(an image, a piece of JavaScript code etc). The web browser while downloading the contents from the target site, is required to send a request to www.B.com to get the third party content. This content coming from the third party site, could also set a cookie - the third party cookie. This cookie belongs to www.B.com and would be sent without notification or requesting permission. The protocol does not require www.B.com to notify the user; furthermore, the web browser does not provide easy mechanism for the ordinary user to manage his privacy setting so as to be left alone.

As mentioned above, a cookie is a text file with a number of attribute-value pairs. The commonly used attributes are: name of cookie, its content, the host(domain), path, for what operations or type of connections is the cookie to be sent and an expiry date. These cookies are stored in a known location and accessible by the browser. The content is usually coded and the user has no knowledge of its value. The cookies are categorized by the domain. User can open the text file corresponding for a cookie and see the contents; some of it is encrypted and not comprehensible. An example is shown in Figure 5.



Information about the selected Cookie

Name: NSC_nz.dpodpsejb.db-ttm
Content: ffffffff87c5c68b45525d5f4f58455e445a4a422970
Host: my.concordia.ca
Path: /
Send For: Encrypted connections only and no script access
Expires: At end of session

Figure 1: Example of a cookie in SeaMonkeys

2.1.4 Cookies and Privacy

Cookies are used by most web applications/service providers to implement the missing state maintenance feature of the HTTP protocol; it is also used to track the users interaction during the users visit to the site. In spite of the rampant use of cookies, as mentioned above, only a small number of web users know about the intent of cookies and a minuscule percent of these explore ways to protect their privacy.

Some web applications may inform users about the purpose of using cookies, others do not. Consequently, it is likely that the users personal information could be tracked without the user being aware of it; this is particularly true with third-party cookies: their purpose is to track users and mine the data for commercial advantage. Third party cookies are set by ad(publicity) networks, analytics platforms, and user behavioural trackers

Cookies, as part of http/https header, can be stolen in the open internet environment; an example of this is a public WIFI without port-isolation configuration.[32] Also, a hacker may use a device to camouflage a public WIFI, with an inviting Service Set Identification (SSID) name such as “GUEST” or “Building_name+FREE”. Once a user signs up through such camouflaged WIFI, the cracker can easily intercept all internet packets, inject JavaScript code which is a basic practice of middleman attack [8].

Also, for some web applications(e.g., a public forum), without adequate input monitoring and filtering (check for and disallow code), a malicious user may acquire cookies belonging to other users by judicious JavaScript code injection. For example, consider a typical PHP based forum software developed. The forum software, may allow user to set their nickname, etc. A malicious user may embed JavaScript code such as:

“WebJunkie$< scriptlanguage = ''JavaScript'' > window.location.href = ''http : //www. * * * *.ca/upload_files/reg.php?var'' + document.cookie; < script >''$

The browser will only show the nickname“WebJunkie” to other users; however, the following code which not shown will send the unsuspecting user’s data who clicks on such a post.

```
<script language="JavaScript">
window.location.href="http://www.****.ca/upload_files/
    reg.php?var"+document.cookie;
<script>
```

The code above gives the basic idea of cross Site Scripting(XSS) attack. This happens when the web application does not filter the user‘s input string carefully, and filter out, e.g., in the example above, the JavaScript code. When users login to the forum and click on this user‘s paste, this malicious JavaScript code would execute which would get and send the reader‘s cookies to the link below:

```
http://www.****.ca/upload\_files/reg.php
```

This XSS attack can collect the cookies from all users who load this malicious post.

3 Privacy Problem: The Cookies Standard

As one notes that the RFC2109 [27] and RFC6265 [28], do not provide a mechanism that allows users to identify what is the purpose of each cookie. Instead, it only states the regulation of the format of cookie and which domain or URL that the cookie belongs to. Meanwhile, there is only syntax regulation for name and value pair in the cookie, so the preference of the methodology of naming a cookie greatly relies on the web application(server) owner. Thus the information of the cookie‘s purpose, type etc. are normally incomprehensible to human or even cookie management tools, which means that, the cookies for each domain, are only readable by the cookie setter. Then, as the consequence to the clients, they only know they are being tracked by specific web application(by URL), however, clients cannot tell what information about them has been recorded, and what actions were tracked. Moreover, due to the lack of knowledge about the cookies, the user agent itself and cookie management add-ons and extensions can only, for a specific domain, delete all the cookies; or not allow any cookies; or allow all cookies. There is no mechanism to control or distinguish the contents of the cookies. From user and privacy point of view, cookies must be classified based on their purpose and the user should be able to allow or reject specific type of cookies!

3.1 User Agent Privacy Facilities

According to Oxford English Dictionary, web browser, is “a program used to navigate the World Wide Web by connecting to a web server, allowing the user to locate, access, and display hypertext documents.” The web browser provides a graphical user interface for user interaction with internet content providers accessed using a specific URL. For example, cbc.ca is the URL for the content provider Canadian Broadcasting Corporation. Nowadays, the web browser, has become not only a tool for web browsing, but also a platform for small, light weight applications running remotely.

However, by taking advantage of such applications the user is handing over his material to these service providers who can do what they want with them according to their fluid privacy policy[1]. Just as an example a privacy policy which runs to many pages can go something like "the service provider can use such data in accordance with our privacy policies .... this would include a worldwide license to use, host, store, reproduce, modify, create derivative works, communicate, publish, publicly perform, publicly display and distribute such content." Furthermore, one is giving them a carte blanche to "automatically analyze the content as it is sent, received or stored, so as to provide personally relevant[2] search results, advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored." Another issue is that there is no legal enforcement that a service provider actually adheres to the rules it says it will comply by!

3.2 Web browser privacy settings

The Platform for Privacy Preferences Project(P3P) was intended to match the privacy of users of the web against the objectives of the website owners to collect information about the visitors to their site. This protocol was never entirely supported and the fact that there was no way to enforce it meant its demise. Most web browsers never implemented the protocol and the protocol is effectively dead.

Web browsers are becoming part of life for most connected users using a multitude of devices. Most of these users are too busy and do not have the time or the know-how to deal with the complexities of the browser. It is thus important that the browsers are truly user agent and not the supplier's agent. Most browsers have an "out-of-box" default setting for cookies. These defaults are shown in the following table.

Most browsers allow some control over the cookies stored on the user's device. The salient difference among these user agents is in the default settings, the ease of use, and the possibility and clarity of implementing whitelist and blacklists. Below are the results of our experiments with these features using the popular user agents in random order.

Chrome(Version 43.0.2357.81 (64-bit)), by default, allows all sites to store local data at the client's site; this is also their recommended setting. The other options are "Keep local data only until you quit your browser" and "Block (all) sites from setting any site data". For third-party cookies and

[1] Part of the policy is that the service provider may modify the policy

[2] Privacy encroaching!

Browser	Allow third-party	Allow first-party	privacy alert
Chrome	YES	YES	NO
Safari	NO	YES	NO
FireFox	YES	YES	NO
Internet Explorer	NO(partial)	YES	NO
Opera	YES	YES	NO
SeaMonkey	YES	YES	YES

Table 1: Default Cookies Settings

site data, chrome marks it as an optional check box and unchecked by default. Which means that it allows third-party cookies by default.

Safari(Version 8.0.6 (10600.6.3)) allows only the website that the user visits to set-cookies. As usual the other options are: block, allow from current website only and always allow. For the default option, it is in line with the statement in the help part of the browser which recommends to accept cookies and website data from visited websites. The default setting would block third-party cookies.

By default, Internet Explorer(IE) blocks cookies but does follow the Compact Platform for Privacy Preferences Project policy and block third-party cookies that save information that can be used without the user's explicit consent. For the first-party as well as the third-party cookie, the user contact information cannot be set without explicit consent.

The default setting in FireFox is to allow ALL cookies including first and third party. Furthermore, it hides many options unless user chooses "Use custom history" setting by going to the Preference and using the Privacy tab to display the much hidden Privacy setting. Many of the options are displayed only when the proper value for the pull down menu next to "Firefox will:" under the History heading is selected. Only if "custom history setting" is selected, FireFox reveals several check box options for browsing and download history, search and form history, accept cookies from sites and clear history when FireFox closes. If "Accepts cookies from site" is checked, FireFox provides two drop down lists for "Accept third-party cookies" and "Keep until". For "Accept third cookies" it has three option: Always; From visited; and never. For Keep until which indicates the cookies expiration setting, the options offered are: "they expire"; "I close FireFox"; and "ask me everytime".

By default, Opera allows all cookies including first and third party and also marks it as recommended. The other options are Keep local data only until I quit my browser, Block sites from setting any data(Block all). Here, Block third-party cookies and site data is a checkbox option which user can only block third party cookies and site data while allowing first party cookies.

By default, SeaMonkey allows cookies(first party and third party). The other options are block cookies(all). Allow cookies for the originating website only(no third-party cookies), allow third party cookies for previously visited websites only. For retention of cookies, it accepts cookies normally by default, the other options are accept for current session only, accept cookies for (user specific) days, and ask for each cookie.

It is troubling to see that the majority of these browsers which have a significant percent of the browser marekt share among them have default setting which allows third party cookies.

3.3 Customization Ability of Major User Agents

Most browsers have some facility to customize the privacy settings. Again the features and the ease of use varies. Most of these allow users to check the detail of each cookie, delete specific cookies or delete all cookies. The ease and details vary with the user agent.

Browser	DO NOT TRACK	BLOCK	ALLOW	CLEAR ON EXIT
Chrome	YES	YES	YES	YES
Safari	YES	ALL/NO	ALL/NO/1st Party	NO
FireFox	YES	YES	YES	YES
IE	NO(partial)	YES	YES	YES
Opera	YES	YES	YES	YES
SeaMonkey	YES	YES	YES	YES(GLOBAL)

Table 2: Default cookies settings

Browser	REMOVE	CHECK DETAIL	BLOCK 3rd PARTY
Chrome	YES	YES	YES
Safari	NO	NO	YES
FireFox	YES	YES	YES
IE	NO	NO	YES
Opera	YES	YES	YES
SeaMonkey	YES	YES	YES

Table 3: Default cookies setting(contd.)

For customizing, Chrome allows creating white-list or blacklist with permission for allowing, blocking and allowing for session(delete on exit - from browser not the site!). For managing cookies, it allows users to examine cookies which re grouped by domains. Also, it allows users to remove a specific cookie or remove all cookies. For warning to server, it allow user to check a check box “Send a do not track request with your browsing traffic” which adds a http header saying that the user does not want to be tracked by the server. As mentioned earlier there is no enforcement of this request by any legal means. Use of a public site of servers that violates this directive may be consulted by the browsers to provide an alert message to the users.

Safari does not have the options for whitelist, blacklist etc. For managing cookies, it allows users to remove all cookies or remove cookies from specific domains. For utilizing cookies, users can add a “Do not track me” header in the http packet by checking the corresponding check box. Opera allows setting exception for cookies; for a specific domain the user can set allow, block and clear on exit: this is a mix of whitelist and blacklist.

FireFox allows blacklist and whitelist in an unified interface. For managing cookies, it allows users to check specific domain’s cookie in detail. Also, it allow user to remove specific cookie or remove all cookies. For utilizing cookiesit allows users to check a “Tell sites that I do not want to be tracked” check box for the sake of adding to http a “Do not track me” header.

Internet Explorer allows the user to specify exception for cookies including ALLOW, BLOCK. For first party and third party cookies, it allows user to accept, block and prompt, also, for cookies to be deleted at the end of a session, it provides a “Always allow session cookies”check box.

Opera allows adding exception regulation for cookies; it can be specific for a domain to be ALLOW, BLOCK, CLEAR ON EXIT(Session cookie), essentially a mix of whitelist and blacklist. For managing cookies, it allows users to check the details of cookies, delete specific cookies or delete all cookies.

For customizing, SeaMonkey provides a different way than the other browsers. In a management console, users can check cookies details, and it provides a box which if checked would not only remove the cookies but also block the domain to set cookies in future; essentially adding the site to a blacklist.

4 Band-Aid Solutions

Since many of the implementers of user agents also have a vested interest in using the consumer data, they are reluctant to enhance the privacy and security features of their products. Over the years a number of third party add-ons have been created by volunteers to address the disappointing lead taken by existing user agents. Many of these efforts started out with a good Samaritan spirit; however, the reality of life with its need to make a decent income meant that some of these add-ons products themselves are moving towards being commercialized into selective privacy data miner accomplices.

4.1 AdBlock Plus

AdBlock Plus is a user agent plug-in for blocking ads, stop tracking and malware domains, pop-ups. It is open source and well-known world wide. AdBlock Plus filtering is based on regular expression to filter specific domains, parameter types. Also, AdBlock Plus allows users to add filter subscriptions. The normal subscription that can be added is EasyList [7]. For stopping tracking, it base on the subscription and built-in database to stop set-cookie and reject domain base on subscription and built-in database. However, according to a recent report [11], the major tracking and ads platform owners and other companies have paid AdBlock to not block their ads. AdBlock also allows non-intrusive publicity to go through while charging others to be put in their Whitelists to be unblocked.

4.2 Ghostery

Ghostery is another add-on and considered to be the ultimate in the "do not track" plug-in aimed at stopping tracking. It shows the user all the tracking that a particular site has bundled with their web contents and allows users to enable any of them. Ghostery now uses an opt-in feature called Ghostrank, which collects anonymous data which could be analyzed and which could create revenue for the company.

4.3 NoScript

NoScript [20] is an add-on for Firefox and allows the user to specify which sites would be allowed to execute scripts such as JavaScript, Java, Flash and others on the browser. Hence scripts from sites not in the whitelist would be blocked. NoScript also provides anti-XSS and anti-Clickjacking protection.

Since currently most websites heavily rely on scripts the user is required to make exceptions which would create a additional work for the user.

4.4 Disconnect

Disconnect [3] is a software based on three technologies: Virtual Private Network(VPN), Redirection and Filter. It stops two ways of tracking, local cookies and server side tracking. Some issues have been reported regarding the response due to the load on their servers.

4.5 Private browsing mode

Private browsing mode is supported by most browsers under different names (InPrivate, private mode...etc). In general, in this mode, the browser will not save cookies, temporary file, form data and other history record. From a user's perspective, it greatly protect user's privacy. However, some users would not find this convenient since it requires re-entering of the data that would normally be stored by the user agent.

5 Possible solutions

5.1 Public-key cryptography

The information stored in a cookie could compromise the user's privacy and hence s/he needs to be aware of its contents. At the same time the user understands that a web server or tracker does not want others to have access to this data.

One possible solution is to use double Public Key Encryption. The server makes its public key accessible and the browser supplies a public key for the user. Contents of the cookie is encrypted by the server using first its private key and then re-encrypted using the user's public key. A user who wants to verify the content of a cookie(before deciding to delete it) has the browser crypt the content using first the private key followed by the servers public key.

5.2 Public blacklists, whitelists

Some of the add-ons mentioned earlier have created blacklists and whitelists. However, they are commercial entities, and do allow entry in the favoured list for a price. Hence it is important that such lists be held by a not-for profit organization. In many countries, there is not much trust in ones handled by the governments so the custodian of such a list is itself an enigma.

6 Conclusion

Most of the user agents are commercial product produced by powerful companies who seem to have a very clear conflict of interest with respect to user privacy. The exception could be considered to be FireFox and Sea Monkey both being under the Mozilla Foundation. However Mozilla Foundation has commercial connection in the form of Mozilla Corporation and according to FAQ associated with the Foundations annual report for 2013 we read that: ”Mozilla’s consolidated reported revenue (Mozilla Foundation and all subsidiaries) for 2013 was $314M (US), as compared to $311M in 2012.” Furthermore, ”The majority of Mozilla’s revenue is generated from search and commerce functionality included in our FireFox product through all major search partners including Google, Bing, Yahoo, Yandex, Amazon, eBay and others. Mozilla’s reported revenues also include very important individual and corporate donations and grants, as well as other forms of income from our investable assets.”

As reported in a recent survey in [16] Americans do not trust their governments nor companies to protect their privacy. This survey concludes that trading their data for personalized service or special coupons is not a good trade-off. At the same time, according to this survey, American feel powerless and resigned and feel they have lost control over their data and companies do what they want with this data. Another problem of the companies knowing the consumer too well is a possibility of differential pricing for different demography. The surprising thing is that people think that if a company has a privacy policy, they will keep their personal information private. These people have not read the so called privacy policy [1] and would be surprised that their data is going into a black hole of traders and miners of data. An example is a privacy policy of a ride sharing company which requires its customer to agree to being traced 24/7 if they agree to connect to their location data once!

Knowing this, it is clear that the ordinary user is left with no choice but to turn to a browser such as Lynx!

The internet via the user agent and web application has become the information highway of this century. It is inappropriate that this highway be controlled by bandits and pirates of centuries past. Highways are public properties and everyone is required to have a safe passage on them without the fear of being robbed. Physical highways are controlled by the public.The information highway must be controlled by the public and thieves must be eliminated. It is time the bent policy makers and politicians wake up. Since technical solutions always have a work-around, strong legal framework must be created and enforced.

References

[1] Bipin C. Desai, “State of Data”, DOI: 10.1145/2628194.2628229

[2] D H Shin, “The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption”, Interacting with Computers, 2010 - Elsevier.

[3] https://disconnect.me/

[4] David M. Kristol, ”HTTP Cookies: Standards, privacy, and politics.” ACM Transactions on Internet Technology (TOIT) 1.2 (2001): 151-198.

[5] Douglas Quenqua, “Facebook Knows You Better Than Anyone Else”, Jan. 19, 2015, http://www.nytimes.com/2015/01/20/science/facebook-knows-you-better-than-anyone-else.html?

[6] DRM, https://www.eff.org/issues/drm

[7] EasyList, https://easylist.adblockplus.org/en/about RFC7540

[8] Franco Callegati, , Walter Cerroni, and Marco Ramilli. ”Man-in-the-Middle Attack to the HTTPS Protocol.” IEEE Security and Privacy 7.1 (2009): 78-81.

[9] http://www.w3.org/TR/2014/REC-html5-20141028/introduction.html#fingerprint

[10] http://www.pcmag.com/encyclopedia/term/43229/first-party-cookie

[11] John Callaham “Report: Google paying AdBlock Plus to not block Google’s ads”, Jul 6, 2013 , http://www.neowin.net/news/report-google-paying-adblock-plus-to-not-block-google039s-ads

[12] http://jingji.cntv.cn/2013/03/15/ARTI1363356067171925.shtml

[13] Jim Handy, “Does the ’Do Not Call’ List Even Work?”, http://www.forbes.com/sites/jimhandy/2013/02/27/does-the-do-not-call-list-even-work/

[14] http://www.w3school.com.cn/js/js_cookies.asp

[15] Joon S. Park, and Ravi Sandhu. ”Secure cookies on the Web.” IEEE internet computing 4.4 (2000): 36-44.

[16] Joseph Turow, Michael Hennessy, Nora Draper, “THE TRADE-OFF FALLACY How Marketers Are Misrepresenting American Consumers And Opening Them Up to Exploition”, https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf, June, 2015

[17] Google, ”Google Terms of Service” April 30 2014.

[18] Lynx the oldest Web Browser, http://lynx.isc.org/

[19] M Ter Louw, J S Lim, V N Venkatakrishnan, “Enhancing web browser security against malware extension”, Journal in Computer Virology, 2008, Springer,

[20] https://noscript.net/

[21] “Online Behavioural Advertising (OBA)”, A report prepared by the Technology Analysis Branch of the Office of the Privacy Commissioner of Canada, Follow Up Research Project, https://www.priv.gc.ca/information/research-recherche/2015/oba_201506_e.asp,June 2015

[22] http://www.oed.com/view/Entry/226695?redirectedFrom=web+browser#eid14802101

[23] Platform for Privacy Preferences (P3P) Project, http://www.w3.org/P3P/

[24] Price waterhouse Coopers LLP, "Research into consumer understanding and management of internet cookies and the potential impact of the EU Electronic Communications Framework", Department for Culture, Media and Sport, April 2011 UK

[25] HTTP State Management Mechanism, Oct. 2000, http://tools.ietf.org/html/rfc2965

[26] http://www.pcmag.com/encyclopedia/term/52849/third-party-cookie

[27] D. Kristol ,L. Montulli.,"HTTP State Management Mechanism" February 1997

[28] A.Barth, U.C. Berkeley., "HTTP State Management Mechanism" April 2011

[29] Tim Berners-Lee, "The Original HTTP as defined in 1991", http://www.w3.org/Protocols/HTTP/AsImplemented.html, 1991

[30] Hypertext Transfer Protocol – HTTP/1.1 1999, http://www.w3.org/Protocols/rfc2616/rfc26165.html, 1999

[31] Tim Berners-Lee, "HyperText Transfer Protocol Design Issues, appro. 1991", archived at: http://www.w3.org/Protocols/DesignIssues.html, 1991

[32] Thomas J. Edsall, et al. "Private VLANs." U.S. Patent No. 6,741,592. 25 May 2004.

[33] Susan Krashinsky, "Privacy watchdog finds targeted ads still too personal", The Globe and Mail, Jun. 15, 2015, http://www.theglobeandmail.com/report-on-business/industry-news/marketing/personal-web-searches-used-to-target-online-ads-privacy-watchdog-finds/article24969469/