Lappeenranta University of Technology
School of Business and Management
Degree Program in Computer Science

Bachelor's Thesis

Jere Kaplas

POSSIBILITIES AND USABILITY OF VARIOUS PRIVACY PRESERVERTION BROWSER ADD-ONS

Examiner(s): Post-Doctoral Researcher Ari Happonen

Instructor(s): Professor Jari Porras

ABSTRACT

Lappeenranta University of Technology
School of Business and Management
Degree Program in Computer Science

Jere Kaplas

Possibilities and Usability of Various Privacy Preservation Browser Add-ons

Bachelor's Thesis

47 pages, 12 figures, 5 tables

Examiner(s): Post-Doctoral Researcher Ari Happonen

Keywords: privacy preservation browser add-on extension plug-in app application security usability tracker cookie personal information adblock

Online privacy is an increasing concern in the modern era where so many things are done over the internet. Many different parties, such as advertising companies, data brokers, and even government agencies use various methods, such as cookies, super cookies, fingerprinting or web caching for tracking users and collecting data from and about them. This paper looks at the possibilities and usability of various privacy preservation add-ons for PC browsers, such as Google Chrome or Mozilla Firefox. Privacy preservation add-ons include add-ons such as Adblock, Ghostery, Disconnect, PrivacyBadger, uMatrix, NoScript or HTTPS Everywhere. Mobile applications were excluded from the study. Privacy preservation add-ons can cause issues or interruptions with normal browsing, this paper looks at some of the issues caused by these add-ons, and possible solutions for improving their usability. Most usability issues originate from lack of information users have, rather than poor application or user interface design.

TABLE OF CONTENTS

1 INTRODUCTION 3

1.1 RESEARCH QUESTIONS 5

1.2 PURPOSE AND SCOPE OF RESEARCH 6

1.3 THESIS OUTLINE 7

2 PRIVACY AND TRACKERS 8

2.1 PERSONAL INFORMATION 9

2.2 TARGETED ADVERTISING AND CONSENT 9

2.3 TRACKERS 11

3 PRIVACY PRESERVATION ADD-ONS 18

3.1 COMMON ADD-ONS 18

3.2 COMBATTING TRACKERS 21

4 USABILITY 26

4.1 PRIVACY CONCERNS 27

4.2 USABILITY ISSUES 27

5 CONCLUSIONS 36

5.1 DISCUSSION 39

5.2 FUTURE RESEARCH 41

6 SUMMARY 42

REFERENCES 43

SYMBOL AND ABBREVIATION LIST

API	Application Programming Interface
DNT	Do Not Track
EU	European Union
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
NIST	National Institute of Standards and Technology
OSN	Online Social Network
PC	Personal Computer
PI	Personal Information
PII	Personally Identifiable Information
RTC	Real-Time Communication
UID	Unique Identification Number

1 INTRODUCTION

Websites collect all manner of data from and about their users. This collecting of data, also referred to as tracking, profiling or targeting, can include collecting the users' personal information (PI). The gathering of data in modern online browsing is widespread and is commonly done for the purposes of advertising. It is important to note that although websites can collect this data by themselves, it is more common that the data collecting is done by or in conjunction with a third party company, commonly an ad agency or a data broker. Data brokers are companies which collect as much data as possible and to sell it to other companies such as advertising agencies, financial institutions, insurance companies, retailer companies, other data brokers or even to government agencies (Federal Trade Commission, 2014).

To better understand how data and personal information is being collected, let us first look at how a webpage is constructed. Websites often include content from many different sources. Any content that a website[1] provides from their own sources is considered first party content. Websites can also include third party sources, meaning a third party will provide content or services, that are integrated onto the website. A common example of this would be ads being provided by a third party ad company.

Third party sources linked to a webpage can contain trackers. Third party tracking technology, referred to as a tracker, is generally a small piece of code which collects data from and about the user. This collected data is associated with users through the use of cookies and other tracking methods. A cookie stores data from the user in a long term data storage, meaning the data is not lost when the browser is closed. As such, a cookie provides a way to save stateful information, allowing trackers to keep records of the users they are tracking. (Mozilla Developer Network, 2016).

Tracking, in particular the use of cookies, is important for the functionality of many websites. For example, cookies make it possible to log in to online accounts or to remember items in online shopping carts. In general cookies provide a way to save and

[1] The distinction between webpage, website and web domain is as follows: Webpage is a single page on a website. Website consists of all the webpages under the same web domain. A web domain is simply the domain name or the URL of a website.

continue online sessions. (WhatAreCookies, 2016). Cookies, or other tracking technologies are not inherently bad or good, they can be used for various purposes. The distinction between using tracking technology for purposes which are important for the functionality of a website are hard to differentiate from third party tracking, more often used for analytical, advertising or some other financial purposes.

Data brokers collect and sell data mostly for marketing purposes, such as advertising and marketing analysis, but also for identity verification or people search. (Federal Trade Commission, 2014). Trackers can collect data about which links are clicked, how long each site is visited, what purchases are made, what topics the user is interested in, etc. This gives tracking companies the means to create a profile on the user, detailing their interests and browsing habits. The use of social media networks, often gives trackers a way to link personal information to this tracking profile. These topics will be discussed in more detail in later chapters.

There is a proposed way to deal with privacy in browsers. Browsers can include a Do Not Track (DNT) request, which is a small piece of information sent (in an HTTP header[2]) to websites when they are loaded. The DNT header requests for the website not to track the visitor. (Mozilla, 2016). Modern browsers commonly have an option to send a DNT request upon accessing a website. The important part is not the technology behind DNT, but the policy. Do Not Track does not prevent tracking. It simply informs the website, that the user does not want to be tracked. DNT Policy is how sites act and respond to the request. Electronic Frontier Foundation has created a DNT policy, which websites can follow when a DNT request is received. But currently there are no legal or technical requirements for websites or advertisers to honor DNT requests or to follow any DNT policy. (Electronic Frontier Foundation, 2016). As such, users currently cannot trust that websites honor their request not to be tracked.

Besides a DNT request, browsers have very limited options for users to protect their privacy. Most include turning off features like cookies, caching[3] or JavaScript completely. Completely disabling such features is not a feasible solution, as in most cases they make it

[2] HTTP header is a part of the Hypertext Transfer Protocol message. DNT is a field in the header, and the field can be set to 1 (opt-out of tracking), 0 (opt-in, allow tracking) or null (no preference).
[3] Caching is a method for temporarily storing web documents on the client, to reduce bandwidth usage.

very hard or outright impossible to use some webpages. Fortunately, there are alternative methods to protecting online privacy from trackers.

The main topic of this paper is about various privacy preservation add-ons. In this context an add-on is a small software application installed on a browser platform. For instance, an add-ons job can be to block third party trackers. Add-ons can also be referred to as extensions, plug-ins or apps. Add-ons can be installed on most modern browsers, including Mozilla Firefox or Google Chrome. The overall theme of the add-ons inspected in this paper is protection of the users' online privacy and security, usually meaning removing advertisements and blocking trackers or harmful scripts. Most of the add-ons researched in this paper have similar goals or objectives: to help users protect their privacy against trackers and other privacy-invading methods, but differ in their methods and scopes of operation. For example, an add-on might only block ads by blacklisting known ad sources, whereas another add-on will block everything by default, working in a so called whitelist mode, where every source and element on a webpage is blocked until the user allows it by adding it to the 'whitelist'.

1.1 Research questions

In order to better understand how these various add-ons can help protect the users' privacy, it is important to examine how these add-ons work. That is why this paper explores the possibilities and limitations of various privacy preservation add-ons, comparing their capabilities to different tracking methods with a focus on usability.

With the primary focus on the usability, the goal was to find out how does usability and required user interaction trade off with protection of online privacy, what are some common usability issues users might face with these add-ons, and how could these add-ons be improved in terms of usability. There are two aspects to consider, the technical and design aspect of how privacy preservation add-ons can be automated, so that required user interaction is minimal, and secondly the human aspect of what are the issues people come across with these add-ons, that could impede the usability. This can be generalized as the main research question: **What are the main causes of usability issues in privacy preservation add-ons?**

To give an example, a simple ad-blocker should not interfere with normal browsing, requiring minimal user interaction. On the other hand, some add-ons require users to constantly decide which domains, scripts or elements of a website are to be allowed and which should be blocked. Such solutions require considerable effort from the user and are far more inconvenient. Yet they provide the user with more control, and thus better security and privacy protection. These types of add-ons frequently block parts of webpages that were important for the webpages' functionality, forcing users to interact with the add-on to fix these situations, which for some users can be frustrating.

1.2 Purpose and scope of research

This thesis should be of some use to both common users and developers of privacy preservation add-ons. The first objective of this paper is to introduce the reader to some of the different methods and privacy issues of data collection and tracking. The second objective present various privacy preservation add-ons and to identify common usability issues users may experience with privacy preservation add-ons. This is done through examination into the methods deployed in the add-ons. Common problems caused by privacy preservation add-ons will be identified, as well as how different add-ons try to solve these problems. In the end there will be speculation on possible solutions to improve these add-ons in terms of usability.

The scope of this research is limited to applications which provide privacy preservation functions in some form. Furthermore, the research is limited to add-ons for PC browser platforms. The main focus of this thesis is on the usability aspect of these add-ons. All of the tested add-ons are available for either Mozilla Firefox or Google Chrome. The inspected add-ons were selected to present a broad variety of different add-ons, based on their scope of operation and different operational models (e.g. whitelisting vs blacklisting) and popularity. This research does not look into privacy preservation on mobile platforms, where the user's ability to protect their privacy is greatly diminished.

The paper assumes reader has some basic knowledge about some of the technical issues discussed, such as how webpages are constructed, basic ideas of caching, workings of the

hypertext transfer protocol, etc. No in-depth knowledge is required, and for the readers' convenience some of these concepts are explained in the footnotes on the pages where the concepts are introduced.

1.3 Thesis outline

This first chapter presented an introduction to privacy issues in modern web browsing, and to the use of trackers and cookies to collect data and personal information from the user. The second chapter will further explain the concepts of personal information, online privacy and the technology behind trackers. The first two chapters serve as a basis for readers to understand the problems with tracking technology and the privacy issues they create, as well as to give an idea as to why third party add-ons are required to deal with these problems. The next chapter will introduce various privacy preservation add-ons, giving detailed explanations of what they are and how they operate. The chapter will show how these add-ons can help protect privacy through more concrete examples as well as showcase what problems they can cause to the user. Chapter four will more closely inspect usability issues within these add-ons, by looking at some of the common problems users of these add-ons might experience, as well as looking at how common the use of these types of add-ons are within different demographics. The fifth chapter will analyze and speculate on some of the causes of usability issues in these apps, as well as suggest some possible solutions and improvements. The final chapter will contain discussion on possible further research on these subjects, a summary of the work and a conclusion to the thesis.

2 PRIVACY AND TRACKERS

To further examine issues of privacy, tracking and gathering of personal information, these concepts have to be defined first. The term privacy is broad and has wide variety of interpretations. Privacy in an online context could be defined as an individuals' ability to protect information about him- or herself. For companies, the important definition of privacy is a legal one, and there are various legal definitions for privacy depending on context. In the context of data collection, the EU defines strict conditions for collecting and storing data about individuals in the Data Protection Directive. The Data Protection Directive states that personal data can only be gathered legally under strict conditions, for a legitimate purpose (EU Data Protection Directive 95/46/EC, 1995). But privacy is not only protected under data protection laws. Many countries consider privacy a universal human right. Under article 8 in the European Convention on Human Right, everyone has the right to respect for private and family life. (European Court of Human Rights, 1950). The European Court of Human Rights has since defined the protection of privacy as a positive right of everyone. (European Court of Human Rights, 2011).

Although the EU has many laws protecting users' online privacy and data, legal requirements for data collection still are not very strict. The requirement for collection data under the EU Data Protection Direct requires that data is collected for a legitimate purpose. A "legitimate" purpose can be as simple and broad as, providing better personalized ads or improving user experience. As such a legitimate purpose does not necessarily need to be in the best interest of the user. There is no legal precedent for websites outside of the EU to follow the EU based data protection directive or e-Privacy directive, meaning EU laws don't necessarily protect users from the EU from websites that are hosted in other countries. (Cookielaw, 2016). Of course that is not to say that all tracking is without cause or that advertising is useless. Advertising is often a necessary mean of monetization for content creators and service providers. The issue of privacy is more considerable when personal information can be linked to the data collected from users.

2.1 Personal information

Personal information, which can be used to identify an individual is referred to as personally identifiable information (PII). PII is defined by the National Institute of Standards and Technology (NIST) as any information about an individual (maintained by an ad agency), which can be used to distinguish an individual's identity. PII includes data such as name, social security number, date and place of birth, even biometric records. Linked PII is any information which can be linked to a person, such as medical, educational, financial or employment records. (NIST, 2010).

If a website has access to any or some of this information it can be used to link a user's tracking profile to their personal information. This information can be obtained from online social networking (OSN) platforms or from online forms, such as surveys, registration, order, payment, or other transaction forms. A research paper by B. Krishnamurthy & C. E. Wills finds that OSN platforms share PII to ad agencies and tracking companies, giving these trackers access to user's name, friends' names, phone numbers, addresses and any other information found on the user's profile. In most cases this 'leaking' of information is an intentional way of sharing PII with third parties. (Krishnamurthy and Wills, 2009).

2.2 Targeted advertising and consent

A major concern of online privacy comes from the lack of consent to tracking. Users generally cannot decline the use of cookies or other tracking methods. Another issue is what the collected data is being used for. For example, PI can be used for behaviorally targeted advertising. The World Privacy Forum (2013) defines behaviorally targeted advertising as the practice of collecting information about consumer's activities, interests and preferences and using that information to serve them with advertisements based on their behavioral record. Tracking companies build a behavioral profile on users, which allows them to serve ads based on the users' interests. For example, a user might search for or visit an insurance company's website and later on receive ads for insurance on other websites. It is understandable that users may want to protect their personal information from being used for such purposes.

When tracking does not require consent, anonymity is hard to preserve. With no real methods to avoid tracking and targeted advertising, being anonymous online has become increasingly difficult. In the EU the e-Privacy directive legislation requires websites to get consent from users to use cookies. Although cookies which are necessary for the site to function are exempt from this requirement, meaning the legislation is mainly directed at cookies used for tracking and advertising.

(EU Personal Data and Protection of Privacy Directive 2002/58/EC, 2002). In practice, this means informing the user that cookies are going to be used. Actually opting-out of these cookies is a different matter altogether, and has not been made easy for the average consumer. Sites often only inform you that they are using cookies, without giving you the option to refuse the cookies on the spot, although some sites do give this option as seen in Figure 1 and 2.

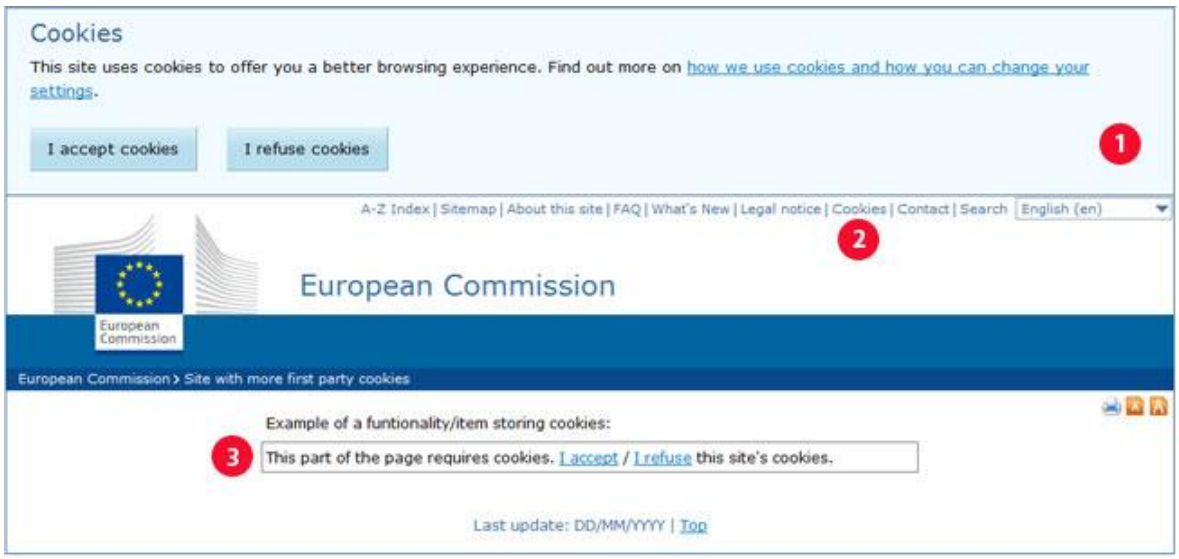

Figure 1 Cookie consent header banner with refuse option

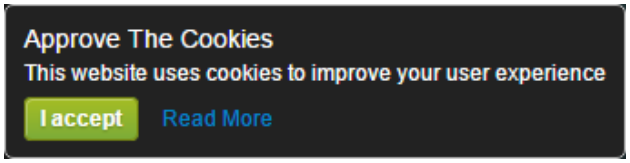

Figure 2 Cookie consent notification without refusal

Instead some ad agencies and tracking companies offer opt-out cookies or add-ons. IBA Opt-out add-on, which is used by Google and Google's partnering sites, opts the user out of "interest based ads". Abine Inc. has created a similar add-on called Targeted

Advertising Cookie Opt-Out (TACO), which automatically opts the user out of various targeted advertising cookies. It is important to note that opting-out like this can be misleading, since often opting-out does not mean stopping tracking altogether, but rather just not showing the user targeted or interest-based ads. Furthermore, these add-ons are unknown to most users and thus not commonly used.

2.3 Trackers

The first chapter talked about using cookies and other methods for tracking. This section is going to look more closely at different tracking methods, to better understand what different privacy preservation add-ons are needed for. Third party tracking was also mentioned quite a few times, and the distinction between third party and first party content or sources is an important one. Most trackers come from third party sources, and the difference is important because usually those sources can be blocked without any repercussions to the functionality of the website, but first party sources cannot be blocked because that would be blocking the very webpage that was being accessed.

Trackers collect data about the sites users' visits, what they read or are interested in, i.e. the users' browsing history. To help with tracking a user, trackers also collect data about the user's device and the device's configuration, generating a device specific fingerprint. (Geary, 2016). To link the collected data with a certain demographic or individual, trackers can try to collect all available PI or PII. As mentioned before, most of this tracking is done by third parties. These third parties are most commonly ad agencies that use the data directly for advertising purposes themselves, or data brokers, companies which collect data for the sole purpose of selling it to other companies or governments. (Browser Tracking). These tracking companies are not related to the sites where their trackers operate, and when their trackers are embedded on multiple sites they are able to track users across the internet.

The most common tracking method is with the use of HTTP cookies, more specifically persistent cookies, also referred to as tracking cookies. Persistent cookies do not expire when the browser is closed, unlike session cookies, instead they expire at a specified date or after a specific length of time determined by the creator of the cookie. Although

persistent cookies have non-tracking applications as well, such as keeping a user logged in even if the session is closed, the persistency allows trackers to log user's activities over a long period of time. Tracking through cookies works by setting a cookie on the user's local machine when they first visit a website. These cookies include a unique identification number (UID). The server side holds a copy of the same cookie, which was set on the user's machine. Every time a user then visits the website any cookies set by that website are requested from the user, allowing them to identify the user from their previous sessions. If no previous cookies are found, a new one will be created. (WhatAreCookies, 2016)

HTTP cookies have limitations, one being their file size. HTTP cookies store information in plain text and can contain up to 4 kilo bytes (KB) of data which in modern computing is not very much (Barth, 2011). HTTP cookies are also relatively easily removed by the user, as browsers allow user to manage their cookies.

HTTP cookies are not the only type of cookie available. Companies have developed their own persistent web storages, similar to cookies, to facilitate their own applications. These storages, commonly referred to as "Super cookies", are often harder to manage and users are often unaware of their existence. Most common example of a super cookie is a "Flash cookie", technically a Local Shared Object (LSO), which is used in Flash applications. Other examples of persistent web storages are Document Object Model (DOM) storage used in HTML5 or Microsoft Silverlight cookies used by Silverlight web applications. (Electronic Frontier Foundation, 2016).

Cookies serve many purposes in tracking and advertising. Cookies can be used to limit the amount of popups users receive or to make sure the same user is not shown the same ad multiple times. (Allaboutcookies, 2016). At the same time cookies can be used to profile the users' preferences and behavior. A paper written at UC Berkley on Flash Cookies and Privacy found that flash cookies often contain the same information stored in the HTTP cookies set by the site, making it harder for users to remove cookies (Soltani et.al., 2009). If a user deletes HTTP cookies, the site that set the cookies could simply copy the same data from a LSO. Unlike typical HTTP cookies, these super cookies never expire and they are not always managed by the browser, making them harder to delete. LSOs are also able

to contain much more data than a typical HTTP cookie, up to a hundred KBs, 25 times as much as an HTTP cookie (Adobe, 2016). The increased storage size allows trackers to more easily collect much more data on the user.

Cookies are not the only way a user can be identified and tracked online. Browsers contain and share a considerable amount of technical information about the user's local machine, and the browser itself. The Electronic Frontier Foundation (EFF) has a research project called Panopticlick, which allows users to test how unique their browser is. The EFF has a list of visible information that browsers gives out. The list as given by EFF includes:

- The user agent string from each browser
- The HTTP ACCEPT headers sent by the browser
- Screen resolution and color depth
- The Time zone your system is set to
- The browser extensions/plugins, like Quicktime, Flash, Java or Acrobat, that are installed in the browser, and the versions of those plugins
- The fonts installed on the computer, as reported by Flash or Java.
- Whether your browser executes JavaScript scripts
- Whether the browser accepts various kinds of cookies and "super cookies"
- A hash of the image generated by canvas fingerprinting
- A hash of the image generated by WebGL fingerprinting
- Yes/no whether your browser is sending the Do Not Track header
- Your system platform (e.g. Win32, Linux x86)
- Your system language (e.g. en-US)

All of this information varies from browser to browser and each of these values can be considered to have a certain amount of bits of identifying information. The bits of identifying information determine how unique a browser is. (Electronic Frontier Foundation, 2015). This identifying information can be considered as a kind of fingerprint, which can be used to identify a specific computer to some certainty. If a website has a previous record of a user visiting their site, they can compare that to the current browser fingerprint to determine if it is the same user. This method of tracking works even if the user deletes their cookies and does not given out any personally identifiable information. Fingerprinting as a method of tracking is almost impossible to avoid. Possibly the best way to avoid tracking through fingerprinting is to use a custom browser, such as Tor: a modified version of the Firefox browser, which among other security and privacy related features, tries to limit the amount of data available for fingerprinting (Tor Project, 2016).

Web cache or caching can be used in different ways for tracking. A web cache is a technology for storing, i.e. caching data for later use. Caching decreases the amount of bandwidth used and can speed up loading times. Much like fingerprinting, taking advantage of the web cache for tracking does not necessarily require the use of cookies or JavaScript. Web cache can be used in various different ways to enable tracking. (Cardwell, 2011). One example makes use entity tags (ETags) to track user's ETag is a part of HTTP caching and provides a way to validate a web cache. In other words, it allows the webserver to know when a user's cache needs to be updated. The webserver can send an ETag with a UID to each browser, and when the browser tries to request the same resource later, it will return that UID, thus allowing the server to track the user. This method works much like cookies, without actually relying on cookies. (lucb1e, 2013). This exchange is depicted in figure 3.

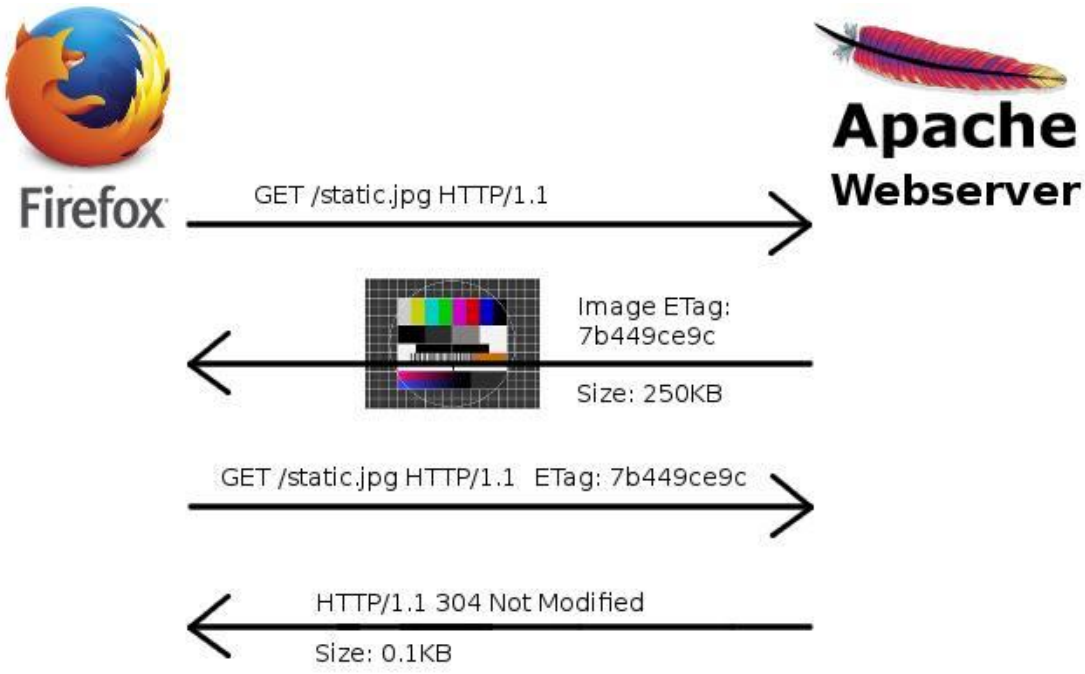

Figure 3 Overview of requesting an image with an ETag from a webserver.

Combining all of these different methods of tracking, makes it nearly impossible to stay completely anonymous. What's more, different sites often contain the same trackers, allowing tracking companies to track users not only on one site, but across multiple sites. This is referred to as cross-site or cross-domain tracking. When multiple sites use the same

trackers, these trackers can get a very good picture of the users' browsing histories. When looking at how many trackers some sites contain, it is not hard to imagine just how much information these trackers are getting. An add-on called Disconnect allows users to visualize third party trackers. As an example, I visited popular software download site, CNET Download, which had over one hundred third party domains attached to it, as seen in figure 4.

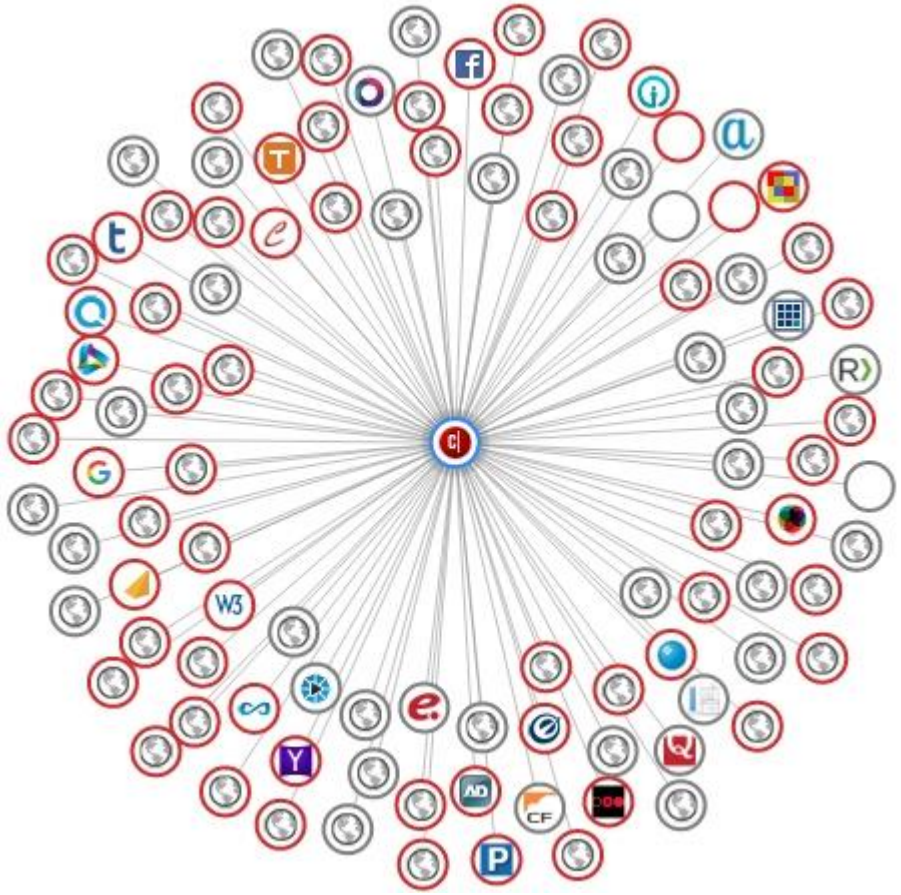

Figure 4 http://download.cnet.com/ third party domains visualized by disconnect.me add-on. Red circles are known tracking sites. Gray circles are not, but may still track you.

One issue with all these trackers is that loading them takes a lot of bandwidth. According to Sarah Downey, an adviser for the privacy company Abine, up to 26% of bandwidth goes to loading trackers (Mitchell, 2014).

Due to the nature of hypertext based design of the internet, protecting ones' privacy is not easily achieved. Websites are dependent on some cookies and JavaScript to function,

making it hard to block only trackers and third party domains that are not integral to the functionality of the website. With super cookies and other means of tracking, modern browsers do not come with the tools to protect the users' online privacy. There are various add-ons that help users protect their privacy, but some are not easy to use and require considerable effort from the users.

To summarize, table 1 includes some of the most common tracking methods, with their basic operations briefly explained. This list is only a handful of all the possible methods for tracking, but most other methods are variations of these and rely on the same technologies.

Tracking method	Basic operation
Storage	
HTTP Cookies	Tracks users through persistent uniquely identifiable cookies set by the webserver on the clients' local storage.
Super Cookies	Also known as zombie cookies, saves same information as HTTP cookies, but relies on technologies such as Flash, Java or Silverlight to save the cookies in a different location. Can be used to restore deleted HTTP cookies.
HTML5 Storage	Uses local storage, i.e. database, to store uniquely identifiable information. This storage is persistent between sessions, and is not cleared when the cache is.
Fingerprinting	
Device, Operating System, Browser	Websites can gather visible information about the configuration of the users' device, operating system and browser, including HTML5 Canvas data. This includes a wealth of data, as detailed in previous list by EFF. Fingerprinting can use a many of different technologies to gather data.
Cache	
Entity Tags	When caching an image, this method stores an ETag with unique information on the client, and when the client sends that ETag back to the server to see if the image has changed, the server can identify the user. Does not require cookies, JavaScript, HTML5 Storage, any plugins or fingerprinting to track users.
Last-Modified Header	HTTP headers include a field called Last-Modified, where a UID could be stored. The UID would then be sent back when the browser requests a same resource from a server later.
Session	
DOM Properties	The Document Object Model has a property called window.name, which can be used to store data.
HTTP Referrer	HTTP referrer header shares information about which page you came from when clicking a link. This information can be made the include data, such as username.

Table 1 Tracking methods and their basic operations summarized

Since there are so many different methods and techniques which can be used to track users online, and it is very difficult to protect one's privacy against them all, not only do users require the assistance of privacy preserving add-ons, but often need multiple add-ons to defend against different threats. Unfortunately, these add-ons do not come without side-effects. Add-ons can cause issues with browsing, and thus requiring users to interact with the add-ons, by changing their settings to solve issues that have arisen. Using multiple add-ons makes the fixing of issues even harder.

3 PRIVACY PRESERVATION ADD-ONS

The previous chapters focused on privacy and different tracking methods. This chapter is going to look more closely at what it means to preserve that privacy and what limitations privacy preservation add-ons might have. Some privacy preservation add-ons are going to be introduced in relation to different tracking methods and explain how they can help users protect their privacy. For an individual, protecting their privacy and personal data can be difficult as there is no one method or add-on which can protect against all the different tracking methods. Furthermore, protecting one's privacy is often done at the expense of convenience and usability. The importance between third party and first party sources should become more apparent as most privacy preservation add-ons are based on blocking third party sources of trackers, but not all trackers come from third party sources. A website can host trackers on its own domain, which is why it's important to look at how different web technologies can be used to tracking.

Privacy preservation add-ons have limitations, they usually focus on protecting against one tracking method, most commonly third party trackers. What add-ons cannot do is stop the users' information from being available in the first place, but they can try to stop trackers from being able to access the information by blocking the sources of trackers. Some types of trackers cannot be blocked by conventional methods, and it is not always possible or feasible to stop websites collecting any data about their users. Instead of blocking data from being collected, privacy preservation add-ons can help stop trackers from associating the collected data with the user. This works if trackers are not able to identify a user from previous sessions or from trackers on other sites. Data that cannot be associated with a specific user is not as useful as it cannot be used to build a tracking profile on the user.

3.1 Common add-ons

Most modern browsers have a vast library of add-ons or extensions available on them. These add-ons extend on the capabilities of the browser, making additional features available. The focus of this paper is on add-ons which in some form provide privacy protection to the user. The rise in popularity of these privacy preservation add-ons is partly due to awareness of the users on how extensive online tracking has become. Some add-ons can show users all the different sources that include trackers. Add-ons such as Disconnect

or Mozilla's Lightbeam allow users visualize all third party domains and trackers on the websites they visit.

The most popular privacy preservation add-ons are ad blockers. Adblock Plus has over a hundred million users, far more than any other add-on available (Protalinski, 2016). The main use for users might be to block ads, but inadvertently or not, these users are protecting their privacy when using add-ons that block ads, since the technology behind blocking ads is the same one used for blocking trackers.

Tracker blockers extend on the same concept that ad blockers use, by blocking all known trackers, not just those that include ads. Add-ons such as uBlock Origin, Privacy Badger, Disconnect or Ghostery all set out to do the same thing, block trackers. These add-ons differ in some of their included features, but also their policy on which trackers to block. By default, most add-ons use lists of known offenders, and block all known trackers based on those lists, this policy, called blacklisting, is the basis of most privacy preservation add-ons. The opposite of the blacklisting policy is to use whitelisting instead. Whitelisting means block all by default, and allow, (i.e. whitelist), as necessary. In reality add-ons usually use some combination of these methods. A great example of combining whitelisting and blacklisting is in the add-on uMatrix, which allows first party sources, but blocks all third party sources by default. In addition, blacklists are also used to block all known tracking sources, unless the user specifically allows them. uMatrix, as the name suggests, uses a matrix, or a table, which consists of rows of domains and columns of elements, which allow users to specify which elements to block from each source. This matrix gives users tremendous control over the content they want to allow or block. Figure 5 shows the overview of the uMatrix interface.

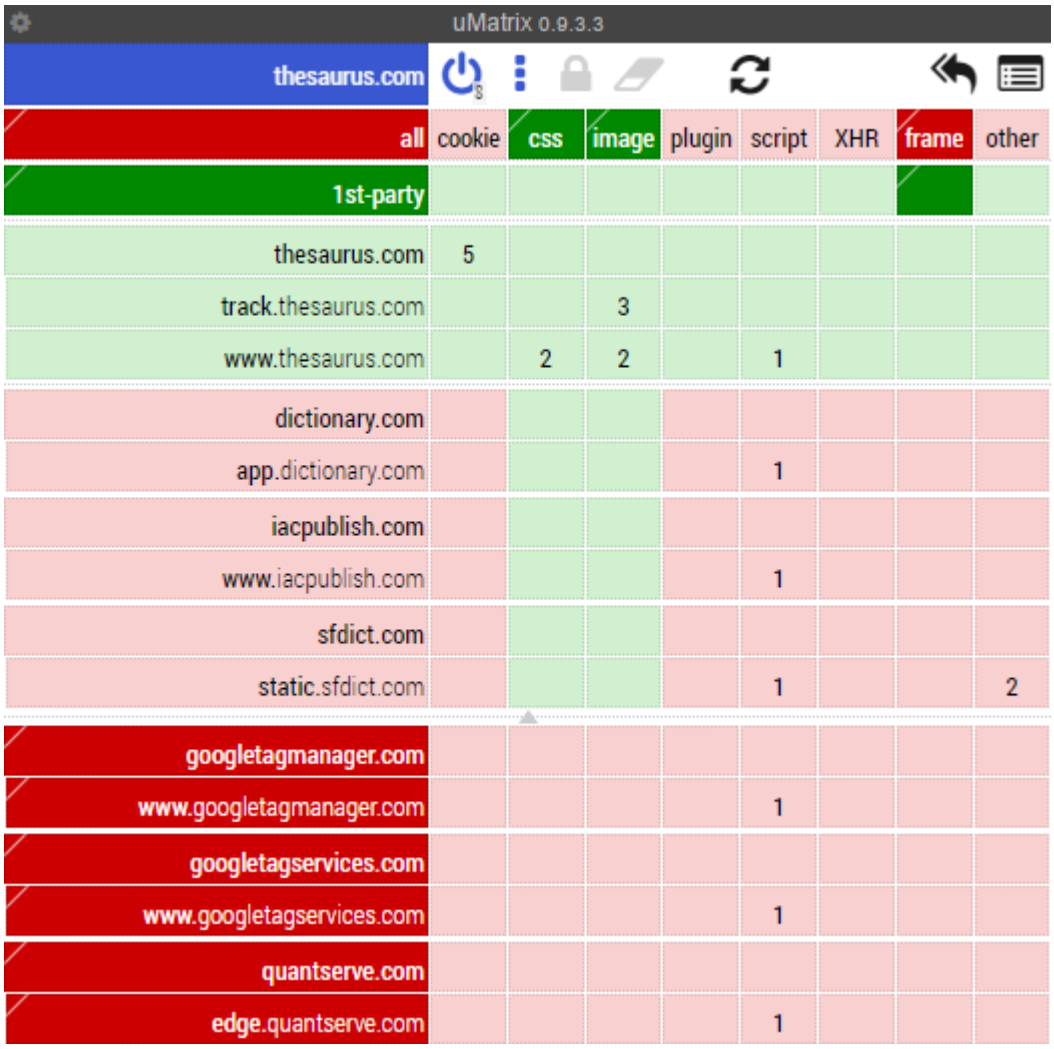

Figure 5 Add-on uMatrix showing all sources separated by different elements on thesaurus.com.

Another approach, used specifically by the add-on Privacy Badger, is to use analysis and heuristic methods to determine whether a third party source is tracking the user, and then block them. Most other add-ons specialize in a certain thing, like NoScript which blocks all JavaScript, Flash, Java and other plugins by default, or BetterPrivacy which gives the user control over their LSOs or Flash cookies.

Table 2 lists all the different add-ons looked at in this paper, and summarizes their basic functionality. This list does not contain all the available privacy preservation add-ons,

Add-on	Basic operation
Adblock Plus	Blocks ads based on filter lists and rulesets based on those lists. Works by blocking the sources of ads before the content is loaded in. Includes acceptable ads list, which is enabled by default but can be disabled.
uBlock Origin	Based on ABP, a generic blocker, blocks ads as well as other known tracking sites. Includes more filter lists which can be enabled in the settings. Also has other privacy preservation settings. Does not have acceptable ads list.
Ghostery	Generic tracker blocker, includes a user interface that shows different trackers by categories. Does not block trackers by default. Based on filter lists.
Disconnect	Generic tracker blocker, blocks trackers by default unlike Ghostery. Similarly categorizes trackers to advertisers, analytics and social sites. Based on filter lists.
Privacy Badger	Does not use predetermined lists, instead analysis third party content for trackers and blocks sites that appear to be tracking users across multiple sites.
uMatrix	Based on same blocking methods as uBlock Origin, but adds a matrix view of all the different domains as rows, and different elements of a webpage as columns. Importantly allows blocking of scripts. Has additional privacy preservation features such as HTTP referrer and user-agent spoofing, as well as automatic deletion of cache and local storage.
NoScript	Blocks Scripts and plug-ins on all sites by default, allowing users to whitelist trusted sites. Only available for Firefox.
HTTPS Everywhere	Forces sites to use HTTPS protocol whenever possible.
BetterPrivacy	Manages LSOs (flash cookies), allowing user to delete them. Only available for Firefox.

Table 2 Common privacy preservation add-ons and their basic operations.

3.2 Combatting trackers

Add-ons are not the only way for users to protect their privacy. Browsers include some ways for users to try to protect their privacy. Some browsers allow the user to send a DNT request when visiting websites, but as mentioned earlier, this is not a reliable method to stop tracking. Most modern browsers also include a private browsing, or incognito mode. Generally private browsing mode stops any history, cookies or cache from being saved, but it will not stop websites from tracking the user, nor does it hide the user's identity. Although in the latest versions of Firefox, private browsing mode also includes tracker blocking, using blacklist provided by the disconnect.me add-on. Users also have control over their browser's settings on things like disabling JavaScript or other features which

could be used to leak the users' data. Users can also delete their cookies or cache, or not save them at all if they wish to.

Another way to make online browsing more secure, without necessarily using add-ons, is to use HTTPS protocol as much as possible when visiting websites. The 'S' at the end HTTPS comes from using the TLS protocol, which stands for Transport Layer Security, sometimes still referred to as Secure Socket Layer (SSL), which was TLS's predecessor. TLS provides secure communication between the web browser (i.e. the user), and the server. Making sure every visited website is using HTTPS can be tedious. That is why users can use an add-on called 'HTTPS Everywhere', which forces the browser to encrypted connection whenever possible.

A step further would be to use a proxy or a virtual private network (VPN) to hide the user's identity. A proxy works by adding server between the user and the web server, through which the users web traffic is tunneled through. This means the website only sees the proxy server, instead of the actual user. VPNs work in a similar fashion, but are more extensive and tunnel the user's entire internet traffic through a VPN server, where as a proxy server is often limited to a certain application or certain type of traffic, such as HTTP traffic only. (Crawford, 2013).

None of these solutions are exactly ideal, as they are not enough to protect the users' privacy on their own, and they either severely limit the functionality of websites or introduce inconveniences that the users then have to deal with. Although these kinds of problems cannot be completely avoided, there are better solutions available.

The most common privacy preservation add-ons, ad and tracker blockers mostly use the same two methods. First is to blocks the users' communication to any server or resource that includes trackers or ads. For example, an add-on might block the user from accessing the web address *"ad.doubleclick.net"*, an advertising agency owned by Google, meaning content from that address will not get loaded, because the request for the content never gets sent in the first place. Secondly, add-ons hide HTML elements, such as images, banners, popups, etc. that are identified as being ads or include trackers. (Adblock Plus).

The way most add-ons, determine whether a web address or HTML element contains trackers, is through predetermined lists, often called blacklists or filter lists. These lists contain rules, for what content should be blocked. Some add-ons, such as Adblock Plus (ABP) contain a list of "acceptable ads", which can be disabled from the add-on's options. These blacklists are maintained different third parties, they get updated frequently and the add-ons automatically apply the updates. Most ad-blockers are very simple to use. For most users the process is as simple as install and forget.

uBlock Origin (uBO), which is based on ABPs' source code, has a different policy on acceptable ads and privacy. uBO filters out all ads by default, and comes with additional filter lists to not only block ads, but also trackers and malware sites. As such uBO describes itself as a wide-spectrum blocker, instead of an ad-blocker. (Hill, 2016). uBlock Origin and other tracker-blockers mentioned in the previous section offer protection against the most common tracking methods, which mostly include the use of cookies, but other possible tracking methods discussed in the previous chapter are still in effect.

Using privacy preservation add-ons can lead usability issues with websites. Websites rely on third party provided content and services and when add-ons block some of those sources, websites can break in unexpected ways. It is not always obvious a website is not working as expected when using an add-on that blocks trackers. Problems do not always arise immediately after vising a webpage. For example, sometimes a problem can appear in the middle of a transaction, or when submitting an online form. These situations can be frustrating, since the user cannot always know if their submission has gone through, or they are forced to refill the form. These problems are caused when an add-on cannot differentiate sources required for a websites functionality or a website requires a third party source that also includes trackers to provide some content or service. To combat such issues, some add-ons use more accommodating methods: less extensive filter lists, acceptable ads, or in the case of the add-on Privacy Badger using analytics to determine whether third party trackers are actually tracking the user.

Privacy Badger tracks all third party domains that make up a webpage. When the same domain appears on multiple sites, it analyzes the source and if it appears to be tracking the user (through cookies, super cookies or canvas fingerprinting), Privacy Badger blocks any further content from being loaded from that source. (Electronic Frontier Foundation). This

solution is much more user friendly and requires less interaction from the user, but as a tradeoff some trackers are going to get through and trackers are not blocked immediately, only after they have been observed to cross-site track the user.

Browsers let users delete their cookies at will, but browser do not always have a way for users to manage super cookies, mainly Flash's LSOs. Chrome deletes other site and plugin data along with cookies, but other browsers like Firefox require add-ons like BetterPrivacy to deal with LSOs. Then there are the tracking methods that do not rely on cookies or super cookies, mainly those that rely on fingerprinting or web caching. The best way to stop tracking through caching is to disable caching in the browser or to frequently delete the browsers local cache. The add-on uMatrix has an option to clear browser cache at set intervals.

There is a trend which can be seen, where a specific technology is being used for tracking, and the way to protect one's privacy is to either disable that technology or in the case of cache or cookies, to delete them frequently. Most tracking methods rely on some scripting language like JavaScript or plugins like Flash, which is why disabling scripts through add-ons like uMatrix and NoScript are very effective at stopping trackers. The most common method against trackers is still to block all known sources of trackers, as there is no need to stop trackers from working, if they are not getting loaded to begin with.

The different tracking methods and how they can be defended against are listed in table 2. This includes methods that rely on add-ons and those that do not require an add-on.

Tracking method	Privacy preservation method
Storage	
HTTP Cookies	Cookies can be set to be removed after the browser is closed, browsers can also only allow first party cookies, or cookies can be disabled selectively or completely. Add-ons can also be used to block known tracking cookies.
Super Cookies	Some super cookies, such as Flash LSOs are deleted when clearing cookies in certain browsers, such as Google Chrome. Others may require an add-on, such as BetterPrivacy to manage LSOs. Super cookies can also be disabled by not using the technologies used to create the super cookies, such as Flash or Silverlight.
HTML5 Storage	HTML5 session and local storages can be disabled in the configuration page of a browser.
Fingerprinting	
Device, Operating System, Browser	Fingerprinting can be lessened by disabling scripts and plugins, such as JavaScript and Flash, which are used to gather information for fingerprinting. Another way is to spoof or fake data about the user's configuration, such as the user-agent string, which identifies the user's browser and operating system and their versions. This can be done in the browsers configuration settings, or by using an add-on, such as uMatrix or User-Agent Switcher. Lastly users can use proxies or VPNs to hide their IP and identity, or use Tor browser.
Cache	
Entity Tags	Entity tags or other caching methods can be avoided by frequently deleting the cache, or by disabling caching altogether. (Note: private browsing modes do not save cache). An add-on, such as uMatrix can also be used to delete the cache at user specified intervals.
Last-Modified Header	Much like entity tags, this tracking method can be avoided by disabling the cache, but also by modifying the headers with an add-on, such as Modify Headers.
Session	
DOM Properties	Although rarely used, this tracking method relies on JavaScript to retrieve data, which means it can be blocked by disabling JavaScript on untrusted sites, with add-ons such as uMatrix or NoScript.
HTTP Referrer	Sending the HTTP referrer field can be disabled in browsers configuration, or by faking it with the Modify Headers add-on. There are also add-ons, such as RefControl which specifically hides the referrer.

Table 3 Tracking methods and how they can be defended against summarized.

4 USABILITY

The previous chapters have alluded to how privacy preservation is a trade off with usability. Privacy preservation add-ons can cause issues with websites as a side effect of blocking certain sources or disabling scripts and plugins. These issues, like missing content, broken functionality or even sites not being able to load at all can cause users to give up on trying to protect their privacy, in favor of a more effortless browsing experience. That is why usability is an important factor of privacy preservation.

Before usability in privacy preservation add-ons is examined closer, let us first define usability in this context. ISO standard 9241: Ergonomics of human system interaction, defines usability as the "extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" (ISO 9241, 2010). For our purposes efficiency is not a major concern. All of the add-ons are relatively small in scale and do not increase or decrease latency or webpage loading times in any noticeable way. The interesting aspects are effectiveness and especially satisfaction. Effectiveness in the context of add-ons is their ability to defend against threats that are in their scope. For example, ad-blockers are expected to block all ads, if some get through, that would be considered a deficiency in the add-ons effectiveness. The main concern about usability is user satisfaction. The concern is not that users will not gain satisfaction from using privacy preservation add-ons, but rather that they will be dissatisfied with their browsing experience because of them. In the end usability is a big factor in any software, especially in something as commonly used as web browsers.

When users encounter problems caused by some privacy preservation add-on, there is a chance they will simply remove the add-on, or disable it for that website completely, instead of taking appropriate steps to solve the problem whilst still maintaining their privacy. That is why it can be assumed that some users who become dissatisfied with privacy preservation add-ons will stop using them.

4.1 Privacy concerns

A 2014 study by PageFair in partnership with Adobe found that 4.9% of all internet users were using some ad-blocker add-on, this corresponds to about 144 million active adblock users. The usage varies hugely depending on demographic, browser or operating system in use. 41% of 18-29 year olds said they use adblock in a poll, whereas people over the age of 45 account for 35% adblock usage. The primary reason for installing ad blocking add-ons was to remove all ads, but 25% of users installed an adblock add-on for privacy or performance reasons. (PageFair, 2014). Another study by PageFair in 2015 show's that ad blocking has increased by 41% in 12 months, increasing from 144 million active users to almost 200 million since the 2014 study. The study also surveyed people who had not used ad blockers before, asking them what would cause them to change their minds. They found that 50% of the respondents listed misuse of personal information as the primary reason to possibly start using ad blocking add-ons. (PageFair, 2015).

The use of ad blocking add-ons is increasing rapidly, and privacy is a concern for users. These studies did not account for other privacy preservation add-ons, but it can be assumed the amount of overall users for all privacy preservation add-ons is even greater. Important thing to note about the findings, is that the largest demographic is young adults, who are interested in gaming, social networking, technology and internet as well as education. These are people who use computers and the internet actively, and for whom learning and using these types of add-ons might be easier. Even though the largest demographic are young adults, they are not the majority if younger and older people are accounted for, this is why usability is an important factor for privacy preservation.

4.2 Usability issues

Websites do not always consider add-ons blocking some of their content in their design, furthermore websites often rely on third party scripts to provide functionality for the site. Privacy preservation add-ons can hide elements and block scripts on a website. A poorly designed website might not deal with the removal of ads or scripts properly, leaving the website malfunctioning in some way. When this happens, it is fair to say the problem was caused by the privacy preservation add-on, even if the site could be made to function properly when these add-ons are used, with better design.

These issues can manifest themselves in various ways. A common issue is content not loading, usually media content such as video, audio or images, but sometimes text as well, it depends on how the website delivers the content. The primary scripting language used on the web is JavaScript, which is commonly used to create some functionality, it can be as simple as changing your language preference on a website, leaving a comment or using some search function or in some cases entire websites are built on JavaScript.

For users to solve problems caused by add-ons, first they have to know a problem exists. Missing content can be obvious and easily noticed, thus it can be solved as soon as the problem is noticed. Problems caused by missing scripts can be subtler, they can be hard to notice until some action is performed which requires the script. For example, a user might be browsing in an online store and they attempt to order something. If an add-on is blocking scripts on the site, that order might not be sent at all. It can be difficult to determine whether some action actually took place, especially for someone who is not familiar with these add-ons or the types of problems they can cause.

Let us look at www.youtube.com for example (figure 6), with the add-on uMatrix enabled with default settings. Default settings for uMatrix allows first party content (i.e. content hosted on the youtube.com domain), as well as any cascading style sheets (css) and images. At first the site looks normal, but as soon as the video is clicked, the problems caused by uMatrix become apparent. The video box, comments and images are not loading, and when attempting to use any functionality, like trying to extend the video description or change the language of the page, it becomes apparent that the buttons and dropdown menus for these are not working either.

Looking at the settings on uMatrix, it can be seen that many different third party websites are being blocked. YouTube relies on these third party sites (owned by YouTube and Google) to provide the content for the website. It is not just media content that is missing, almost all functionality besides normal html links have stopped working.

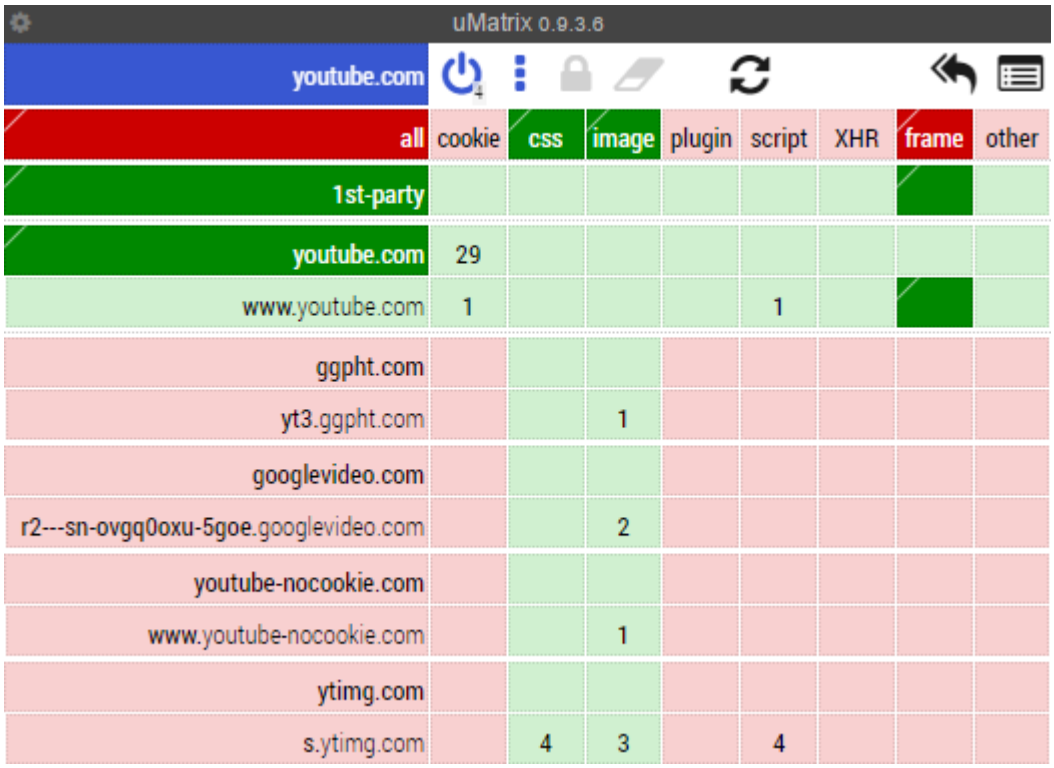

Figure 6 uMatrix settings on www.youtube.com

Once various domains displayed in figure 6 are allowed, the website starts functioning again: videos are loading, images are being displayed, all the functions that required scripts are now working correctly. Looking at uMatrix again (figure 7), it can be seen that a lot more content has loaded in, and the newly loaded content is now blocked. The dark red domains have been explicitly blocked, as they are known sources of ads and trackers. Not all domains needed to be unblocked to get the website to work properly, and therein lies the problem, how to tell which domains should be allowed and which should be blocked?

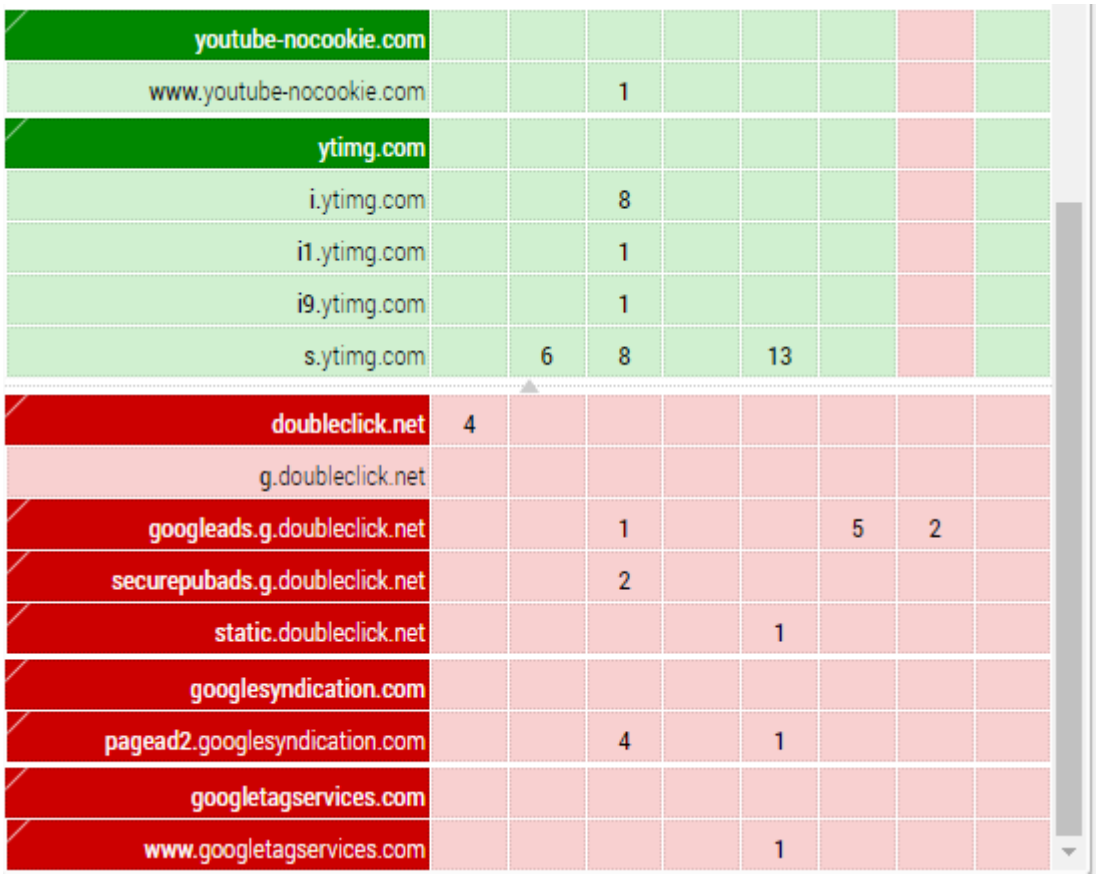

Figure 7 uMatrix on www.youtube.com after allowing some third party domains.

Other add-ons, such as NoScript cause similar issues. The reason these types of add-ons can be problematic is that they operate in a whitelist mode, meaning everything except first party content is blocked by default and needs to be whitelisted. Most other add-ons operate in a blacklist mode, which allows all content by default and only blocks content specifically blacklisted. These add-ons commonly come with predetermined lists of known advertising and tracking sites.

The real problem is not that add-ons using whitelist mode require more user interaction, since they are fairly simple to use, and can be learned very quickly. The difficult part is in distinguishing which domains should be unblocked or allowed to make the site functional, without permitting sites that could track the user. As seen in the example with figures 6 and 7, these sites or domains often have very abstract and abstruse names such as “ytimg.com” or “ggpht.com”. Currently these add-ons have no indication as whether these sites are safe to unblock.

One way is to simply search for the names of these sites. There is plenty of information available online to find out what these sites are for, and if they are safe to unblock. Sometimes the name can be an indication as well, “img” in the name is usually for image server, a server where the site hosts all their images, “cdn” stands for content delivery network. With time and repeated use of these add-ons, common third party content delivery sites pop up frequently and can be globally allowed. Globally allowing domains means as the user allows more and more sites, they start to build their own ruleset, and once their most frequented sites and most frequent third party content delivery domains are allowed, they will counter problems less and less frequently.

It is clear to see that add-ons like uMatrix and NoScript require a lot of work from the user. These add-ons are for people who want to have greater control over their privacy and security, at the cost of ease of use. There are other add-ons, which try to protect the user’s privacy without requiring constant user interaction. Most add-ons, such as Adblock Plus, uBlock Origin, Ghostery and Disconnect simply work in the blacklist mode, only blocking known tracking and ad sites. As such, users do not have to change any settings in the add-on, except in some rare cases where a website does not function with these add-ons enabled. Some sites, commonly video streaming sites can also require that ad-blocking add-ons are disabled.

Add-ons like Adblock Plus, Ghostery and Disconnect allow the user to choose which blacklists to use. They have some lists enabled by default, but Adblock Plus for example does not block all ads, they have a list of what they call acceptable ads, which the user can disable to block all ads. Other add-ons have similar options. uBlock Origin for example has options to block known malware sites, on top of the usual privacy and ad related domains, as well as blacklists or filters for specific regions and languages, as shown in figure 8.

Figure 8 Add-on uBlock Origin Settings

One add-on, Privacy Badger, takes a different approach. Instead of using a predetermined blacklist, it analyses sites the user visits to determine whether there are any trackers or not. More specifically Privacy Badger looks for third party domains, that have been detected on multiple sites, to see if they are cross-site tracking the user. If a site is detected to be a tracker, it is automatically blocked. [https://www.eff.org/privacybadger]. Privacy Badger has some flaws as well. If a site uses trackers from first party sources, or from a source the user has not encountered before, the trackers will not be blocked. Even for the most common trackers, it takes a while before Privacy Badger catches on and starts blocking them. This automatic approach is effective in the sense that it does not require a list, and more importantly it does not require anyone to constantly update that list to block trackers, but at the same time it is vulnerable to some trackers.

Privacy Badger is a perfect example of the balance between privacy and usability. It offers ease of use, a mostly uninterrupted browsing experience, but it can be less effective than traditional add-ons which use blacklists, or add-ons like uMatrix, which block all third

party content. Although there is this contrast between these add-ons, does not mean it has to be a choice between one or the other. The add-ons can be used in conjunction to combat trackers more effectively.

Combining add-ons can have a lot of benefits, but also disadvantages. Let us take a few aforementioned add-ons for example. uBlock Origin, a general purpose blocker, Privacy Badger, a tracker blocker that works by analysis instead of filter lists and HTTPS Everywhere. These add-ons have the same ultimate goal, the protect the users' privacy and security, but they perform different functions. uBlock Origin blocks known tracking, advertising and with some tweaks other malicious sites and sources. Privacy Badger does not use lists of known offenders, but it has the advantage of blocking trackers that for some reason might not be on those lists. HTTPS Everywhere does not block trackers at all, but it does force the user's browser to use encrypted connections (HTTPS vs HTTP) everywhere it can. All of these add-ons can work well together, blocking and protecting the user from different threats.

Most privacy preservation add-on cause some kind issues, as they are fundamentally disruptive to the normal state of websites. When using multiple add-ons, the problems that users might face become increasingly complex to solve. Instead of just having to figure out how to make a site work again with one add-on, now the user has to first figure out which add-on is causing the problem, or if multiple add-ons are causing issues. It could be that two add-ons are causing the same issue, meaning the user has to adjust both. Even though users can further increase their security by using multiple add-ons, it comes as a further trade off with usability.

Table 4 summarizes different privacy and usability concerns of the different add-ons from table 2. Table 5 provides an overview of the different usability issues with privacy preservation add-ons, categorized by effectiveness, efficiency and satisfaction. This is a brief overview into complicated issues, where there are no absolute solutions.

Add-on	Privacy and Usability Concerns
Adblock Plus	Includes a default acceptable ads list. Default list of ads / trackers is fairly limited. Can only be disabled for entire page.
uBlock Origin	Has additional privacy features, but they're hidden in options. Allows disabling of blocking for certain domains only, but this option is enabled for advanced users only.
Ghostery	Does not block trackers by default. Has proprietary lists of trackers (no custom lists supported). Collects data about users and which sites they block by default.
Disconnect	Uses proprietary filter lists (no custom lists supported). Has very limited user settings.
Privacy Badger	Blocking is automated, but does not block all trackers, only blocks sites it after finds them to contain trackers.
uMatrix	Blocks known trackers explicitly, like uBlock Origin but also blocks all third party sites until they're white listed, thus requires much more user interaction. Has many privacy preservation features, but they're hidden away in the options. Much more complex to use than other add-ons.
NoScript	Similar to uMatrix blocks everything by default, requires user to whitelist trusted sites. Only available for Firefox.
HTTPS Everywhere	Only works on sites that provide HTTPS (TLS). Can cause problem with loading a site that should have HTTPS, but for some reason doesn't work at the moment.
BetterPrivacy	Can only delete set cookies, does not prevent them being set in the first place. Only available for Firefox.

Table 4 Privacy preservation add-ons and concerns about their usability and privacy.

Usability issue	Possible Solution
Effectiveness	
Add-on doesn't block all threats	There is no one in all add-on that can protect against every tracking method. That's why users can and should use multiple add-ons if they're concerned about their privacy. In addition, users should configure their browsers to such settings, that they meet their privacy preservation needs, as well as learn browsing habits that help protect their privacy.
User doesn't know what add-on does or how it works	Add-ons should be designed in such a way that they can be used in a simple manner, but if additional or important hidden features exists, users should be informed of these at least when they first install the add-on. A simple introductory page that explain the basic operation and features of the add-on could be helpful for most users. An example could be user not knowing that the add-on Ghostery doesn't block trackers by default, if left uninformed, the add-on would give nothing more than a false sense of security.
User doesn't have easy access to information	Sometimes users don't know which sites are safe to unblock, or which settings should be used. For example, access to information about domains could be improved by including search features in add-ons, especially those which allow users to allow/block third party domains. Sharing information between add-on's users could also be facilitated within the add-on. These problems also lessen with experience and time. Add-ons which require users to allow content become easier to user with the as the user's personal ruleset of allowed domains grows.
Efficiency	
Add-on slows down browsing	Most add-ons are lightweight and can even speed up browsing, as they lessen the amount of content that needs to be loaded. Some add-ons are more efficient than others though. For example, uBlock Origin has been shown to be more efficient in terms of memory and processor usage than other similar add-ons, such as Adblock or Adblock Plus. Users should aim to use only the necessary add-ons they need, and if efficiency is still a problem, look for better alternative add-ons.
Add-on is slow to use	Add-ons should be designed so that they can be used with minimal effort, and so that they're automated as much as possible. If an add-on requires user interaction it should be done in a way that requires as few steps as possible from the user.
Satisfaction	
Add-on is hard to use	This comes down to the previous issues. Add-ons should be easy to operate, have a user friendly interface and provide users with necessary information about settings and possible decisions they have to make. If an add-on is complex by design, users need to consider their technical capability and willingness to use such add-ons.
Add-on causes annoyances	Add-ons are disruptive to browsing, and as such can cause many different issues. Users should choose add-ons that they're willing to setup and operate, rather than using an add-on that's a constant grievance. Developers of add-ons can improve satisfaction by dealing with some of the previously mentioned issues, such as a good user interface, access to necessary information and automating the process as much as possible.

Table 5 Usability issues and possible solutions to them

5 CONCLUSIONS

Privacy preservation add-ons have different kinds of issues associated with them, but they are mostly not related to poor user interfaces. The usability issues often rather come from lack information. User's simple do not know about the different options in the add-ons, they might not know what the different settings do, making it hard to solve issues caused by the add-ons. In the case of add-ons like uMatrix or NoScript, user's might not know what different domains are used for, making it hard to decide which ones to block and which ones to allow. These issues are further complicated by having multiple add-ons installed.

Add-ons have to cater to a large user base, who have different needs and expectations. That is why it is important that users have settings to configure the add-ons to work for them. A lot of users who start using these add-ons simply "install and forget", and add-ons can have unexpected default settings. For example, as mentioned previously, Adblock Plus does not block non-intrusive ads by default, and the add-on Ghostery does not block anything by default. It would be helpful if add-ons to had some introduction page, when the add-on is installed, to inform users about some of the settings and limitations of the add-on. Some add-ons have this have some kind of introductory page, but many still do not.

Most add-ons, especially ad blockers try to be simplistic, they usually can either be turned on or off for a specific website, but other than that there are not many different settings. Some add-ons such as Disconnect or Ghostery (as can be seen in figures 9 and 10) visualize the blocked sources, making it easier for users to see what is happening behind the scenes, and possibly making it easier to solve any arising issues. Notifications about blocked sites can be helpful for noticing and fixing problems, but they can also be an annoyance to more experienced users, as such add-ons should support enabling or disabling such features at the user's will.

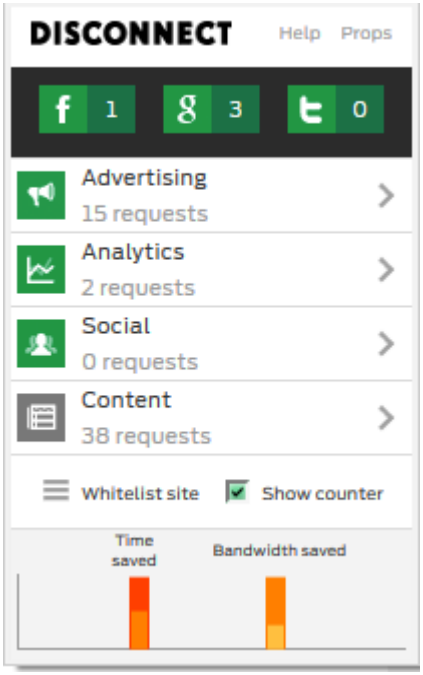

Figure 9 Disconnect add-on UI

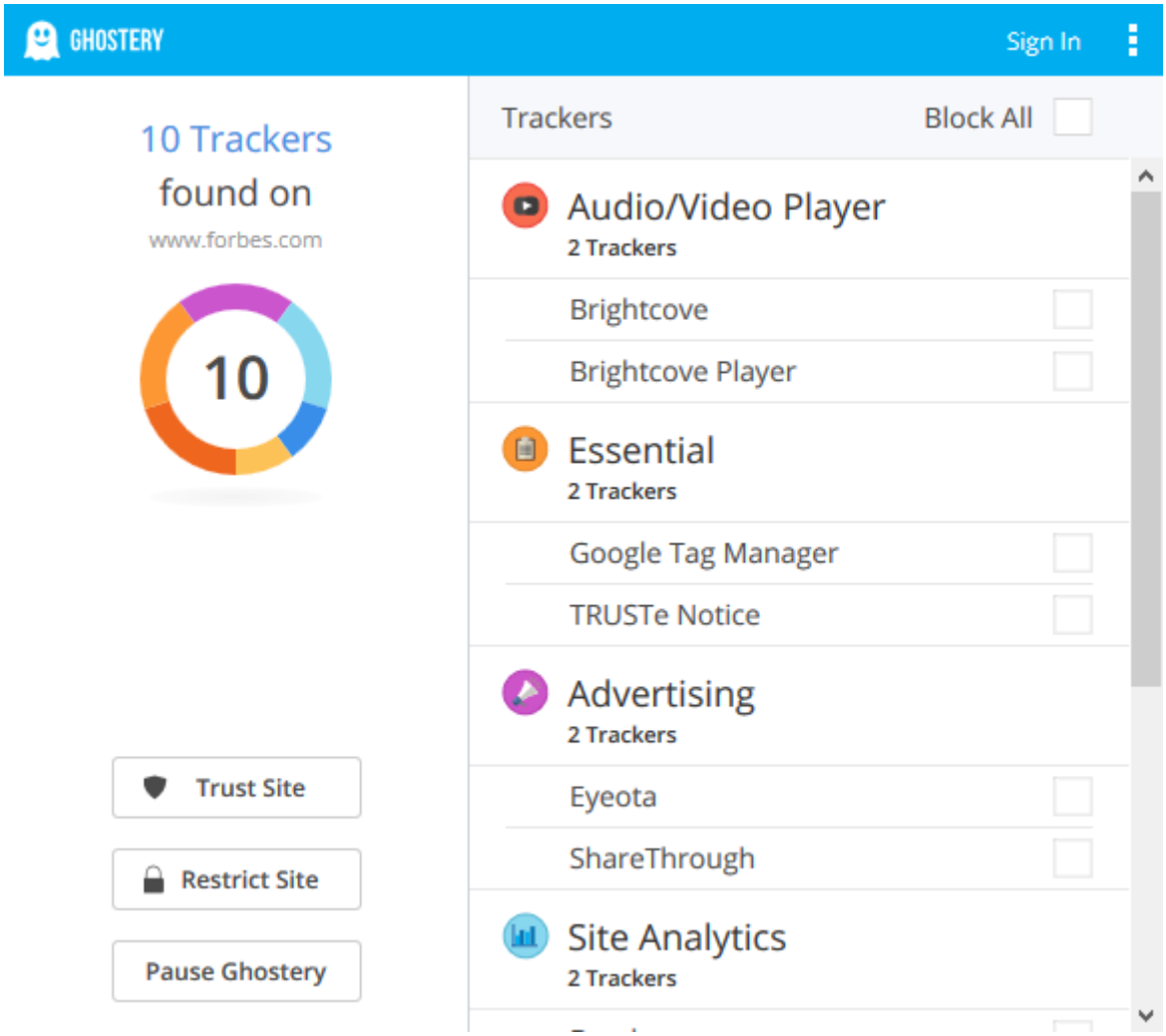

Figure 10 Ghostery add-on UI

The add-on Privacy Badger is somewhat unique in the sense that it inspects and analyses third party sources and cookies to determine whether they contain trackers. If a user wants to also use have a blacklist that filters out already known tracking sources, they'll have to turn to a different add-on. Furthermore, Privacy Badger doesn't block any first party sites, meaning if the tracking is done by the same site the user is visiting Privacy Badger becomes useless. According to EFF Privacy Badger has some kind of first party privacy protection plans (Electronic Frontier Foundation, 2016). If and when these become a reality remains to be seen.

For add-ons such as NoScript and uMatrix the main issue is about knowing which domains are safe and how to find that information. Currently there's no indication what all the different domains are used for and if they might contain trackers. Users can often find information about a domain simply by searching for it in any search engine, but this can be tedious and time consuming manual work. This process could be made easier for user's by implementing two features. Firstly, a way to quickly search relevant information about a domain, speeding up the process, and secondly a rating system that could show the community's opinion on how safe a certain domain is. The rating system could be some kind of indication in the UI of the add-on, and any user could "vote" or give their assessment of the domain. This could even be automated to show how many percent of users have unblocked that domain. This would allow new users to more easily gauge how safe a domain is to unblock. Figure 11 depicts one such possible solution in a mockup.

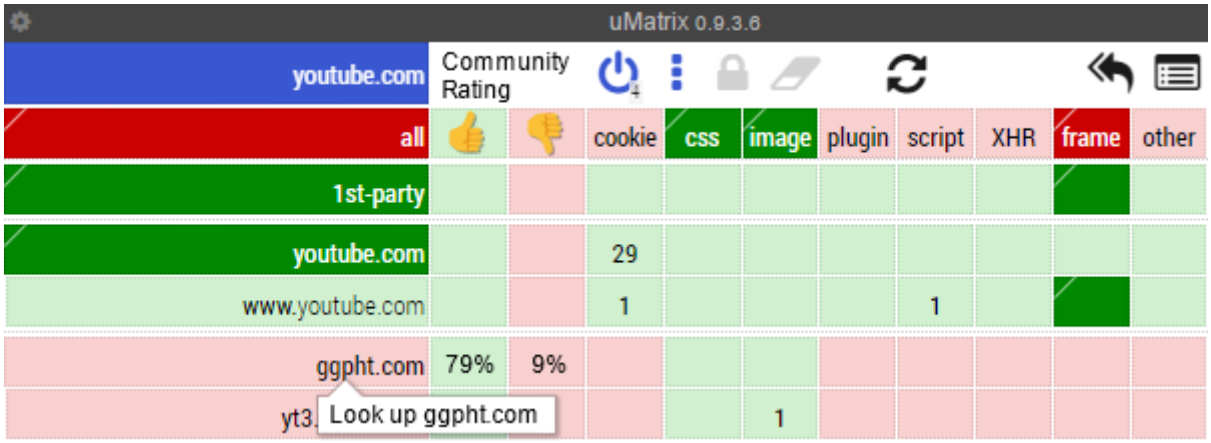

Figure 11 Add-on uMatrix mockup concept

The same idea of making information more available can be applied to most add-ons. It is simple more prevalent in add-ons that require more use interaction. Utilizing the community to improve these add-ons, and providing the community with a way to help each other is something that could improve the usability of these types of add-ons significantly. By sharing information users could make better informed decisions, leading to users unblocking fewer malicious sites.

5.1 Discussion

It can be difficult to know which add-ons are best suited to protect one's privacy. I made a simple activity diagram, figure 9, to help choose from some of the possible privacy preservation add-ons. This is only one possible simplified solution, and in reality it comes down to preference and how valued privacy is over convenience.

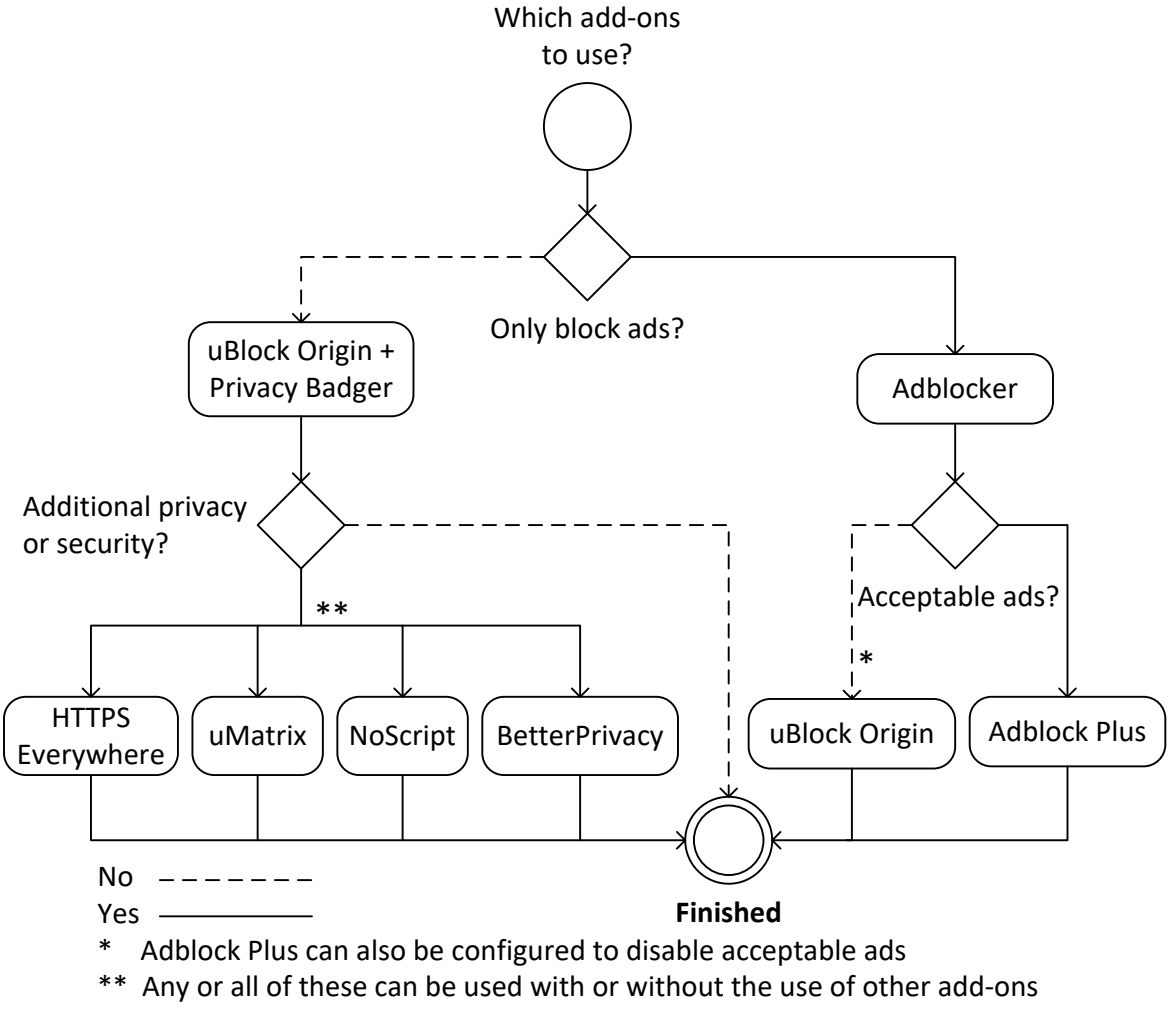

Figure 12 Activity Diagram for choosing add-ons

Most of the available add-ons are generic and can be configured to work the same way, the biggest difference is in the default settings and operating mode of these add-ons. Adblock Plus for example supports acceptable ads, but has an option to disable them, whereas uBlock Origin does not support acceptable ads at all. For someone who likes to fiddle with the different settings, deciding which add-on to use isn't a big issue, but for those, and for the majority of users, who simply prefer to install and forget, the default settings matter. Most people might not be aware that Adblock Plus is still allowing some ads to be displayed. I would not recommend using more add-ons than necessary. Using multiple add-ons that do the same thing, for example uBlock Origin and Adblock Plus, does not necessarily increase protection, but it does make solving any issues harder.

The goal is to allow as few source as possible without allowing trackers to get through. If an add-on is a constant hindrance, it can be tempting to simply allow the entire website or to disable the add-on completely. That is why it is better to choose add-ons that the user has the endurance to keep using. For most users I would recommend uBlock Origin as it blocks all ads, but also other known trackers and malicious sites, the options also include filter lists for specific countries. For casual users Privacy Badger is a great addition, as it's not based on the same filter lists as most other add-ons. HTTPS Everywhere is also a another add-on which serves a different purpose, but can be vital for protecting the users' online privacy.

For people who privacy is a critical issue, add-ons like uMatrix and NoScript can give greater control over the content they want to allow. It has to be noted that these add-ons require much more work to use, and that is why I would not recommend these add-ons for novice or casual internet users. Add-ons alone cannot fully protect their privacy or identity. If the primary objective is to block ads, trackers, increase performance or to stop targeted ads, these add-ons are well suited for that. If the goal is to be completely anonymous, these add-ons can help, but the user is more than likely going to have to use a proxy or a VPN. More information about online privacy and different tools on protecting online privacy, not only in browsers but other applications as well, can be found at www.privacytools.io.

5.2 Future research

This paper focused on inspecting different tracking methods, how users can protect themselves against those trackers, and how the usability of privacy preservation add-ons could be improved. There are many different methods that can be used for tracking, and many different add-ons to combat those tracking methods. For this reason, I think there should be research into the possibility of combining add-ons, or rather creating new privacy preservation add-ons that could combat different tracking methods in an 'all-in-one' solution.

Another area of research could be into solutions for allowing ads without compromising privacy, right now most privacy preservation add-ons also block ads, not because they set out to block ads, but rather because ads often contain trackers. ABP's acceptable ads list is one possible solution to this problem, but the possibility of a more automated, technical solution should be appealing to both users who only care about privacy, not ads, and to advertising companies.

To further continue improving usability of privacy preservation add-on, by including easier access to information and crowd-sourcing information sharing to the community could be prototyped into some of the add-ons, such as NoScript or uMatrix which are both open source.

6 SUMMARY

Privacy is an increasing concern in the online world. There are many varying laws that protect users' privacy at least at some level, but these laws don't give users' right to complete anonymity and they cannot keep up with constant technological advancements. Modern browsers don't provide users with the ability to protect their privacy completely, and the privacy protection possibilities that they do have are hard to use and can severely limit the functionality of websites, making browsing on the internet generally much more cumbersome.

Online tracking uses a multitude of different methods to gather data from and about users. These methods include the basic HTTP cookies, but also super cookies and other tracking methods that are even more invisible to users, methods that do not even require JavaScript to be enabled, methods that take advantage of the vulnerabilities in the many different technologies used in the modern world wide web.

There are many different add-ons that help users protect their privacy. These add-ons have their strengths and weaknesses, but no single add-on is able to protect a user's online privacy completely. Users can install and use multiple add-ons at once, which is recommendable, but can lead to arising problems becoming more complex to solve.

Although most add-ons are fairly simple to use, requiring minimal user interaction, using multiple add-ons means solving an issue caused by an add-on becomes harder, at least if the user intends to solve it in a way that doesn't compromise their privacy. This is because it cannot be impossible or at the very least difficult to tell where a problem originates from. Herein lies the problem, users simply cannot always know the cause of a problem, thus making problem solving at best educated guessing. Most usability issues originate from lack of information, rather than poor UI design or other such cause.

To improve the usability of privacy preservation add-ons, these add-ons could improve access to information, possibly by making it possible to share information between the community.

REFERENCES

Adblock Plus. *FAQ - Adblock Plus internals.* [online] Available at: https://adblockplus.org/faq_internal [Accessed 18 Mar. 2016].

Adobe, (2015*). ActionScript® 3.0 Reference for the Adobe® Flash® Platform: SharedObject.* [online] Available at: http://help.adobe.com/en_US/FlashPlatform/reference/actionscript/3/flash/net/SharedObject.html [Accessed 2 Apr. 2016].

Allaboutcookies, (2016). *How does third-party ad serving work?* [online] Available at: http://www.allaboutcookies.org/ad-serving/ [Accessed 21 Nov. 2016].

Barth, A. (2011). HTTP State Management Mechanism. [pdf] U.C Berkley: Internet Engineering Task Force. Available at: https://tools.ietf.org/pdf/rfc6265.pdf [Accessed 9 Sept. 2016].

Cardwell, M. (2011). Preventing Web Tracking via the Browser Cache. [online] Grepular. Available at: https://grepular.com/Preventing_Web_Tracking_via_the_Browser_Cache [Accessed 11 Sept. 2016].

Cookielaw.org, (2016). *Cookie Law FAQ.* [online] Available at: https://www.cookielaw.org/faq/ [Accessed 17 Nov. 2016].

Crawford, D. (2013). Proxies vs. VPN – What's the difference? [online] BestVPN. Available at: https://www.bestvpn.com/blog/4085/proxies-vs-vpn-whats-the-difference/ [Accessed 4 Sept. 2016].

Electronic Frontier Foundation, (2016). *A privacy-friendly Do Not Track (DNT) Policy.* [online] Available at: https://www.eff.org/dnt-policy [Accessed 21 Nov. 2016].

Electronic Frontier Foundation. (2016). *New Cookie Technologies: Harder to See and Remove, Widely Used to Track You.* [online] Available at: https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide [Accessed 20 Nov. 2016].

Electronic Frontier Foundation, (2016). *Privacy Badger.* [online] Available at: https://www.eff.org/privacybadger [Accessed 13 Aug. 2016].

European Court of Human Rights, (1950). European Convention on Human Rights. [pdf] Council of Europe. Available at: https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Convention_ENG.pdf [Accessed 4 Sept. 2016].

European Court of Human Rights, (2011). Internet: case-law of the European Court of Human Rights [pdf] Council of Europe. Available at: http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf [Accessed 4 Sept. 2016].

European Parliament and of the Council of 24 October 1995, (1995). EU Data Protection Directive 95/46/EC. [pdf] Official Journal of the European Communities, Article 6.1. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN [Accessed 3 Mar. 2016].

European Parliament and of the Council of 12 July 2002, (2002). EU Personal Data and Protection of Privacy Directive 2002/58/EC. [pdf] Official Journal of the European Communities, Article 5.3. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML [Accessed 10 Mar. 2016].

Federal Trade Commission, (2014). *Data Brokers: A Call for Transparency and Accountability.* [pdf] Federal Trade Commission. Available at: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [Accessed 3 Sept. 2016].

Geary, J. (2016). Tracking the trackers: Introduction to cookies and web tracking. [online] the Guardian. Available at: https://www.theguardian.com/technology/2012/apr/23/cookies-and-web-tracking-intro [Accessed 20 Nov. 2016].

Hill, R. (2016). uBlock Origin Blocking mode. [online] Available at: https://github.com/gorhill/uBlock/wiki/Blocking-mode [Accessed 22 Mar. 2016].

ISO 9241. (2010). *Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems.* [online] ISO. Available at: https://www.iso.org/obp/ui/#iso:std:iso:9241:-210:ed-1:v1:en [Accessed 11 Sept. 2016].

Krishnamurthy, B., Wills, C. E. (2009). On the Leakage of Personally Identifiable Information Via Online Social Networks. [pdf] Barcelona: ACM. Available at: http://conferences.sigcomm.org/sigcomm/2009/workshops/wosn/papers/p7.pdf [Accessed 21 Mar. 2016].

lucb1e, (2013). *Cookieless cookies.* [online] Lucb1e. Available at: http://lucb1e.com/rp/cookielesscookies/ [Accessed 11 Sept. 2016].

Mitchell, R. L. (2014). Ad tracking: Is anything being done? [online] Computerworld. Available at: http://www.computerworld.com/article/2489106/data-privacy/ad-tracking--is-anything-being-done-.html [Accessed 3 Apr. 2016].

Mozilla, (2016). *Do Not Track* [online] Available at: https://www.mozilla.org/en-US/firefox/dnt/ [Accessed 30 Aug. 2016].

Mozilla Developer Network, (2016). *HTTP Cookies.* [online] Available at: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies [Accessed 27 Aug. 2016].

My Shadow. *Browser Tracking.* [online] Available at: https://myshadow.org/browser-tracking [Accessed 9 Sept. 2016].

National Institute of Standards and Technology, (2010). Guide to Protecting the Confidentiality of Personally Identifiable Information. [pdf] Gaithersburg: National Institute of Standards and Technology, U.S. Department of Commerce. Available at: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf [Accessed 20 Mar. 2016].

PageFair, (2015). *The cost of ad blocking.* [pdf] Available at: https://downloads.pagefair.com/wp-content/uploads/2016/05/2015_report-the_cost_of_ad_blocking.pdf [Accessed 11 Nov. 2016].

PageFair, (2014). *Adblocking Goes Mainstream.* [pdf] Available at: https://downloads.pagefair.com/wp-content/uploads/2016/05/Adblocking-Goes-Mainstream.pdf [Accessed 11 Nov. 2016].

Panopticlick, (2016). *Panopticlick Is your browser safe against tracking?* [online] Electronic Frontier Foundation. Available at: https://panopticlick.eff.org/ [Accessed 3 Apr. 2016].

Protalinski, E. (2016*).* Adblock Plus passes 100 million active users. [online] Available at: http://venturebeat.com/2016/05/09/adblock-plus-passes-500-million-downloads/ [Accessed 26 Aug. 2016].

Soltani, A., Canty, S., Mayo, Q., Thomas, L. & Hoofnagle C. J. (2009). Flash Cookies and Privacy. [pdf] UC Berkeley School of Law, University of California, Berkeley. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862 [Accessed 21 Mar. 2016].

Tor Project, (2016). *Anonymity Online*. [online] Available at: https://www.torproject.org/ [Accessed 11 Sept. 2016].

WhatAreCookies. *What are Cookies: Computer Cookies Explained.* [online] Available at: http://www.whatarecookies.com/ [Accessed 17 Nov. 2016].

World Privacy Forum, (2011). *Behavioral Advertising and Privacy.* [online] Available at: https://www.worldprivacyforum.org/2011/03/resource-page-behavioral-advertising-and-privacy/ [Accessed 18. Mar. 2016].

Figures

Figure 1. European Commission. *Cookie consent header banner with refuse option.* [image] Available at: http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm [Accessed 10 Mar. 2016].

Figure 2. Cookie-script. (2016). *Cookie notification without refusal.* [image] Available at: https://cookie-script.com/ [Accessed 10 Mar. 2016].

Figure 9. lucb1e, (2013). *Overview of requesting an image with an ETag from a webserver.* [image] Available at: http://lucb1e.com/rp/cookielesscookies/etags.jpg

[Accessed 11 Sept. 2016].

Figure 4. Disconnect.me Add-on. *Third party domains visualized by disconnect.me add-on.* [image] Available at: http://disconnect.me [Accessed 18 Mar. 2016].

Figures 5, 6, 7. uMatrix Add-on. [image] Available at: https://github.com/gorhill/uMatrix [Accessed 3 Sept. 2016].

Figure 8. uBlock Origin Add-on. [image] Available at: https://github.com/gorhill/uBlock [Accessed 4 Sept. 2016].

Figure 9. Disconnect.me Add-on. [image] Available at: https://disconnect.me/ [Accessed 20 Nov. 2016].

Figure 10. Ghostery Add-on. [image] Available at: https://www.ghostery.com/ [Accessed 20 Nov. 2016].

Figure 11. uMatrix Add-on mockup. [image] Available at: https://github.com/gorhill/uMatrix [Accessed 21 Nov. 2016].

Add-ons

Adblock Plus. Version. 1.12.4. Chrome. Available at: https://adblockplus.org/

BetterPrivacy. Version. 1.77. Firefox. Available at: https://addons.mozilla.org/en-US/firefox/addon/betterprivacy/

Disconnect. Version. 5.18.23. Chrome. Available at: https://disconnect.me/

Ghostery. Version. 7.1.0.49. Chrome. Available at: https://www.ghostery.com/

HTTPS Everywhere. Version. 2016.11.8. Chrome. Available at: https://www.eff.org/https-everywhere%20

NoScript. Version. 2.9.5.2. Firefox. Available at: https://noscript.net/

Privacy Badger. Version. 2016.9.7. Chrome. Available at: https://www.eff.org/privacybadger

uBlock Origin. Version. 1.9.16. Chrome. Available at: https://github.com/gorhill/uBlock

uMatrix. Version. 0.9.3.6. Chrome. Available at: https://github.com/gorhill/uMatrix