Cookie Blocking and Privacy: First Parties Remain a Risk

German Gomez [A][E], **Julian Yalaju** [B][E], **Mario Garcia** [C][E], **Chris Hoofnagle, JD**[D]

Florida International University[A]

Syracuse University[B]

Texas A&M University-Corpus Christi[C]

UC Berkeley School of Law[D]

Team for Research in Ubiquitous Secure Technology (TRUST) 2010[E]

University of California, Berkeley

Berkeley, USA

Abstract

HTTP cookies are small files that can make surfing the web faster and more convenient. They can allow sites to recognize returning users so that they can avoid repetitive log in procedures when they visit their favorite sites. Although these type of cookies can be beneficial, they can also be used by third parties to track users. When a user visits a domain and cookies are set on their machine directly from that site's server, these are called first-party cookies. When a third-party site sets cookies on this same domain, these are referred to as third-party cookies. Many of these third-party cookies are used to track user activity as they navigate within the domain and even when they leave to visit other domains. In the past few years, the five major shipping browsers have all implemented new privacy settings to help stop users from having their activities tracked.

In this paper, we describe our investigation of the effects of cookie blocking and privacy. We conducted two experiments to determine the effectiveness of cookie blocking in different browsers. Our first experiment was to collect raw statistics from all five major browsers while visiting all of Quantcast's top 100 sites. We wrote a code in Python that opened all 100 pages at once in each browser, and then counted the number of cookies that were set, prevalence of each cookie name and the number of unique domains that set cookies. We ran this experiment with third-party cookies blocked and unblocked to compare the difference in each browser. Our second approach was an analysis of traffic to get a closer look at the exchange of cookies between our machine and different web servers using

Wireshark. When we opened individual packets, we were able to locate the source IP addresses and domain names that the cookies originated from so we could tell who was setting cookies.

In our numerical results, we found that tracking cookies make up about 25% of all of the cookies set throughout our testing. Through traffic analysis, we found that third parties are finding alternative ways to set cookies on user's machines by making them appear as first party cookies. That being said, we can say that many first party cookies could still potentially be trackers.

I. Introduction

The computing industry has been changing rapidly over the past two decades because of the ongoing development of the internet. Because of the growing complexity of web applications and the stateless nature of HTTP (Hypertext Transfer Protocol), the HTTP cookie was created to store textual information that a web application can use to identify clients and provide a state of information. A cookie is a small text file stored on a user's computer. Cookies are employed for a variety of reasons including enhancing user's online experience by helping sites recognize users when they return. By recognizing users each time they return, cookies can help by storing information such as a password or simple preferences so that users don't have to go through a repetitive process each time they want to visit one of their favorite sites. (1)

Although cookies can make things more convenient for users, they also raise a privacy issue. A common distinction must be drawn between first-party cookies and third-party cookies. (2) The former is issued by the website the user is visiting; the latter by a completely different website. Third-party cookies (Third-party cookies) are commonly used to track users across different websites, usually for analytics or advertising purposes. Thus for privacy-sensitive users, blocking third-party cookies is seen as a convenient and effective way of preventing tracking by advertising and other companies without disabling the basic functionality of the web. (3)

Although blocking cookies may benefit consumer privacy, it is detrimental to analytics companies, since it can skew data that is essential to maintaining their business model. A recent ComScore study showed that frequent cookie deleting and rejection by users can result in more than 2.5 fold inflation of unique users. (4) To ensure the integrity of their data, many analytics and advertising companies are beginning to find ways to bypass the blocking of third-party cookies. According to a study by Web Trends Inc. (A global web analytics company) many companies have begun to set their third-party cookies as first-party cookies in order to keep their analytics as accurate as possible. (5) In addition to these first-party tracking cookies, there are also a few other ways that sites are bypassing the blocking of third-party cookies. Setting third-party cookies in JavaScript allows for the cookie to be set at run time and the cookie value can be sent back to the third-party server, so the cookie is set within the page and looks like a third party cookie. DNS aliasing can also have the same masking effect, because it can make a third-party server appear as if it is part of the first-party server. (6)

Our motivation in this research was to answer a few questions about third-party cookies and the effects of blocking them. First we wanted to find out if blocking third-party cookies was sufficient for users to avoid being tracked by third parties. With this data, we wanted to also find whether or not third-party cookies were still relevant to analytics and advertising companies, and if the distinction between first and third party cookies still mattered. If there were cookies that were able to still track users even with third-party cookies blocked, this would mean that the distinction between parties would be irrelevant because third parties would have to use different methods of setting third-party cookies.

II. Background

Cookies have raised public concerns on internet privacy because they can be used to track and build user profiles. In addition, some cookies could contain additional personal information. Yue [20] developed an extension to Firefox named CookiePicker that automatically validates the usefulness of cookies from a web site and set the cookie usage permission on behalf of users. A Web page is automatically retrieved twice by enabling and disabling some cookies. If there are obvious differences between the two retrieved results, cookies as classified as useful; otherwise, they are marked as useless. CookiePicker reduces privacy and security risks.

Informed consent indicates that the consent a person gives meets certain minimum standards. For a person to give informed consent, he needs to have and understanding of the facts, implications, and future consequences of an action. The person should be in possession of all relevant facts at the time consent is given. Friedman(13) researched the importance of informed consent in Web-based interactions, focusing on the way cookies are managed in the Web browser.

Click fraud is a common attack on Internet advertising. Advertising contributes to the support of the Internet by covering the some expenses of the content publishers' sites. Some publishers use packets generation tools or automated clicking links tools to attack competitors. Metwally(17) developed a method to detect these attacks based on counting cookies.

III. Methods

Two separate methods were used in collecting data in this research. In a practical approach to solving our problem we split our experiment up into two sections. Section one was a statistical approach in which we gathered raw data from browsers while using privacy settings as a variable. Section two analyzed the exchange cookies between our machine and web servers using a traffic analysis tool.

Cookie Counting

In our research, we analyzed the five major shipping browsers and a representative sample of 100 websites. According to W3School (7) the five most popular web browsers are Internet Explorer 8, Firefox 3.6, Opera 10.6, Google Chrome 5.0 and Safari 5.0. To test these browsers, we used Quancast (8) to provide us a list of the top 100 websites by volume in the U.S for the month of July.

The behavior of cookies will be analyzed when third party cookies are blocked and when they are allowed. Figure 1 below shows the procedure we will follow for each one of the cases in which third-party cookies are blocked and unblocked.

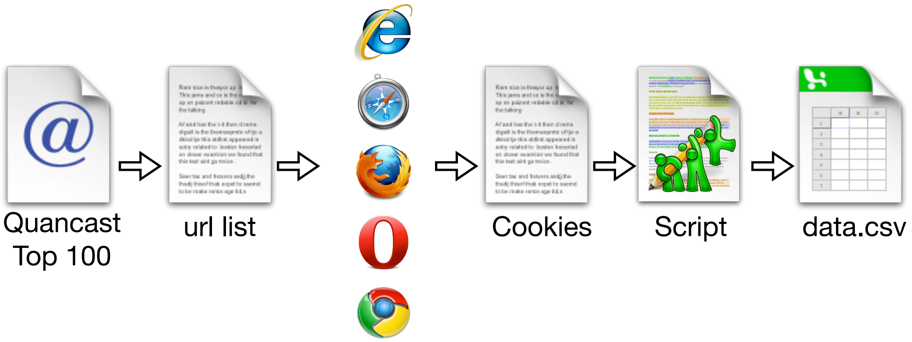


Figure 1: Cookie counting flowchart.

Testing:

Testing was performed on a Macbook Air Mid 2009 running Mac OS X 10.6.4 and Windows 7 on its boot camp partitioned.

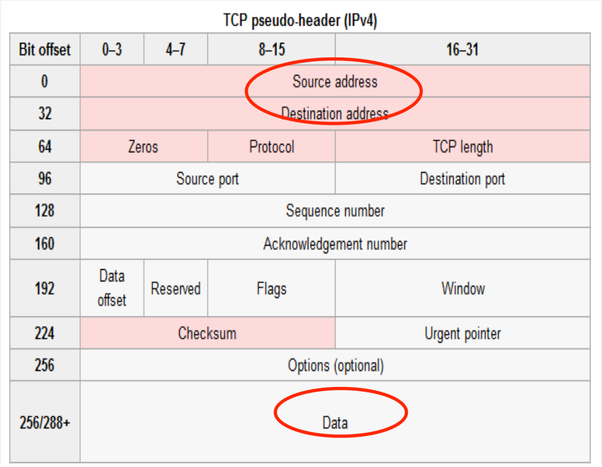
Steps. To ensure the consistency and integrity of the data a series of steps will be followed in order to keep consistency between browsers and operating systems.

1. All operating systems were updated to ensure all security measures were applied.
2. A bookmark~~s~~ file was created for all browsers. The top 100 websites had been split into five groups of twenty.
3. Flash Website Storage will be deleted from the online utility from macromedia http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html
4. Cookies and temporary files were removed from all browser before testing
5. Verify that the Cookie settings were in either accept all, or block 3rd party cookies.
6. Visit the Top 100 websites in groups of 20 to ensure not to crash any browser.
7. Before closing the websites, we will collect the cookie information and save it on a secondary location for further analysis. Closing the browsers before collecting the cookies will yield the loss of session cookies.
8. Custom scripts were developed ~~for~~ to count each cookie.
9. Run script and collect data.
10. Data Analysis.

Traffic Analysis Methods

Wireshark Graph Analysis: After counting the cookies set in each browser with different privacy settings, we were able to perform a traffic analysis of our machine using Wireshark. Wireshark is a traffic sniffing tool that allows the user to see all traffic coming in and out of their computer. We used the Quantcast top 100 sites and wrote a script in Python that opened all of the pages one by one in Firefox (with Third-party cookies blocked). To only view packets containing cookies, we used the filters “http.set_cookie” and “http.cookie” in Wireshark, which showed only cookie traffic entering and leaving the computer. As the pages opened, Wireshark would capture the filtered packets in an IO graph into two separate lines (incoming and outgoing). Each time a page was done loading, the script would wait 10 seconds to ensure that all data was exchanged and then close the page and proceed to the next one. This way, the packet data between individual sites would not be mixed. Since the x-axis in the Wireshark graph used time as a unit of measurement, we kept a graph key that has a time value on the x-axis for each of the top 100 sites. Once we had the graph, we saved it as a .PNG image and were able to analyze further from there.

Packet Analysis: After finding the sites that had the most traffic, we did a packet analysis of these sites using Wireshark. In Wireshark, users can look inside TCP packets and find data such as the source address, the destination address and the data stored in the body text. In the body of the text we were able to see the domain that the cookie came from, as well as expiration dates and any additional values the cookie contains. Figure 2 shows the structure of an IP packet.



TCP pseudo-header (IPv4)

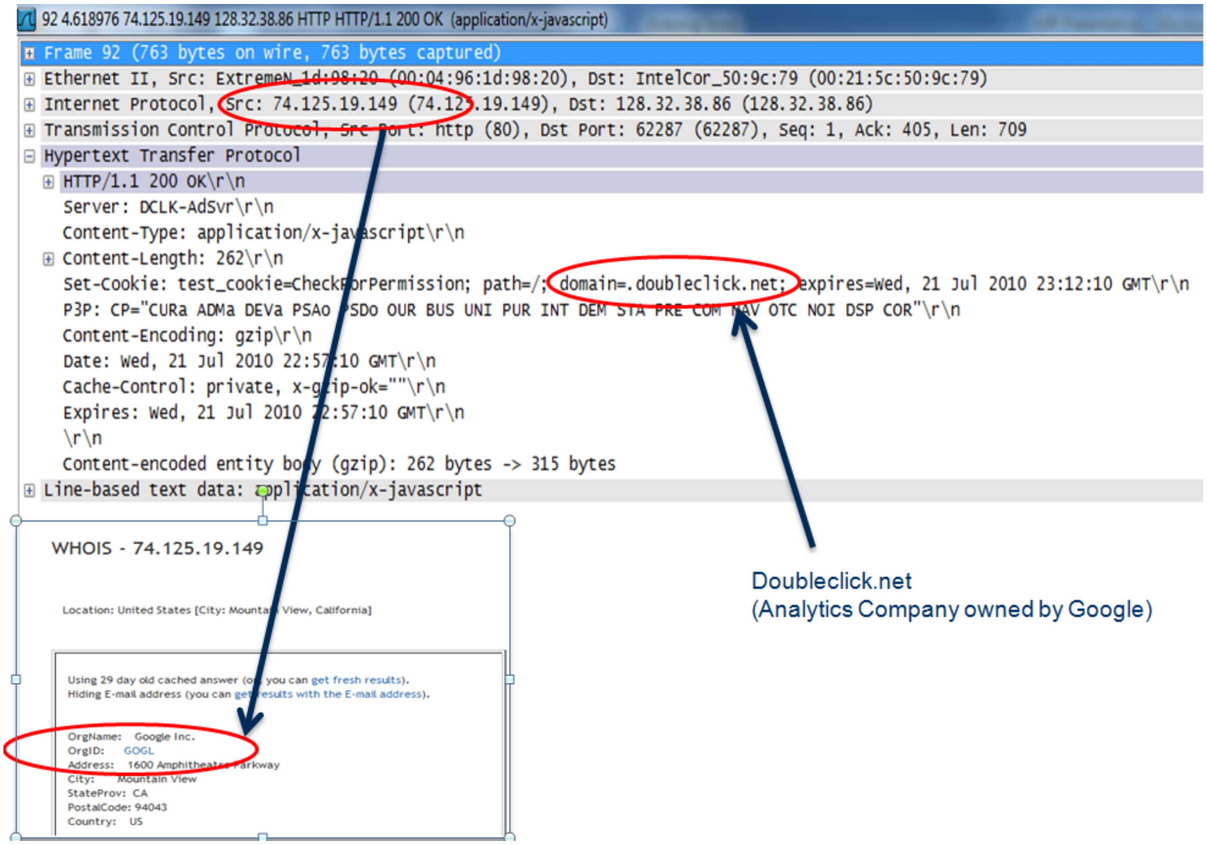
Bit offset	0–3	4–7	8–15	16–31
0	Source address			
32	Destination address			
64	Zeros		Protocol	TCP length
96	Source port			Destination port
128	Sequence number			
160	Acknowledgement number			
192	Data offset	Reserved	Flags	Window
224	Checksum			Urgent pointer
256	Options (optional)			
256/288+	Data			

Figure 2: Contents of a TCP packet

IV. Results and Discussion

After our analysis of the IO graph from Wireshark, we found that there is still a large amount of data sent back to each website servers, even with third-party cookies blocked. The IO utility revealed that even on sites that set fewer cookies, the amount of data sent back to the servers is greater than the original amount.

In our packet analysis we were able to look at the individual packets sent back and forth from our computer and the different web servers. In figure 3 a screenshot of Wireshark shows us the source IP address and domain which the packet came from. What we found was that many cookies were still being set in JavaScript by third parties, but they were set directly on the first party site. Therefore they are considered first party cookies by Firefox. This means that some sites have found a way to bypass the blocking of third party cookies and continue to track users for analytics and/or advertising purposes.



```
92 4.618976 74.125.19.149 128.32.38.86 HTTP HTTP/1.1 200 OK  (application/x-javascript)
⊞ Frame 92 (763 bytes on wire, 763 bytes captured)
⊞ Ethernet II, Src: ExtremeN_1d:98:20 (00:04:96:1d:98:20), Dst: IntelCor_50:9c:79 (00:21:5c:50:9c:79)
⊞ Internet Protocol, Src: 74.125.19.149 (74.125.19.149), Dst: 128.32.38.86 (128.32.38.86)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 62287 (62287), Seq: 1, Ack: 405, Len: 709
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.1 200 OK\r\n
    Server: DCLK-AdSvr\r\n
    Content-Type: application/x-javascript\r\n
  ⊞ Content-Length: 262\r\n
    Set-Cookie: test_cookie=CheckForPermission; path=/; domain=.doubleclick.net; expires=Wed, 21 Jul 2010 23:12:10 GMT\r\n
    P3P: CP="CURa ADMa DEVa PSAo PSDo OUR BUS UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"\r\n
    Content-Encoding: gzip\r\n
    Date: Wed, 21 Jul 2010 22:57:10 GMT\r\n
    Cache-Control: private, x-gzip-ok=""\r\n
    Expires: Wed, 21 Jul 2010 22:57:10 GMT\r\n
    \r\n
    Content-encoded entity body (gzip): 262 bytes -> 315 bytes
⊞ Line-based text data: application/x-javascript
```

WHOIS - 74.125.19.149

Location: United States [City: Mountain View, California]

Using 29 day old cached answer (or, you can get fresh results).
Hiding E-mail address (you can get results with the E-mail address).

OrgName: Google Inc.
OrgID: GOGL
Address: 1600 Amphitheatre Parkway
City: Mountain View
StateProv: CA
PostalCode: 94043
Country: US

Doubleclick.net
(Analytics Company owned by Google)

Figure 3: Wireshark showing cookies.

Blocking third-party cookies does reduce on average 40% the number of cookies on the browser as seen on figure 3 A 2:1 relationship between the number of unique cookie name and the unique cookie domain was observed. However, despite blocking third-parties cookies, we found that tracking cookies are still present in the form of first party cookies. The Results in figure 4 represent a detail view from Apples' Safari 5.0 web browser. In our domain analysis we found there were some cases when third-party doubled the number of cookies set on the Among the top cookie names were the following: __umta , __qca and s_vi. These cookies belong to companies like Google, Quancast and Omniture. In spite of the fact that blocking third-party cookies reduces by 40% on average, it was found that tracking cookies make up more than 25% on average from the total number of cookies on this test.

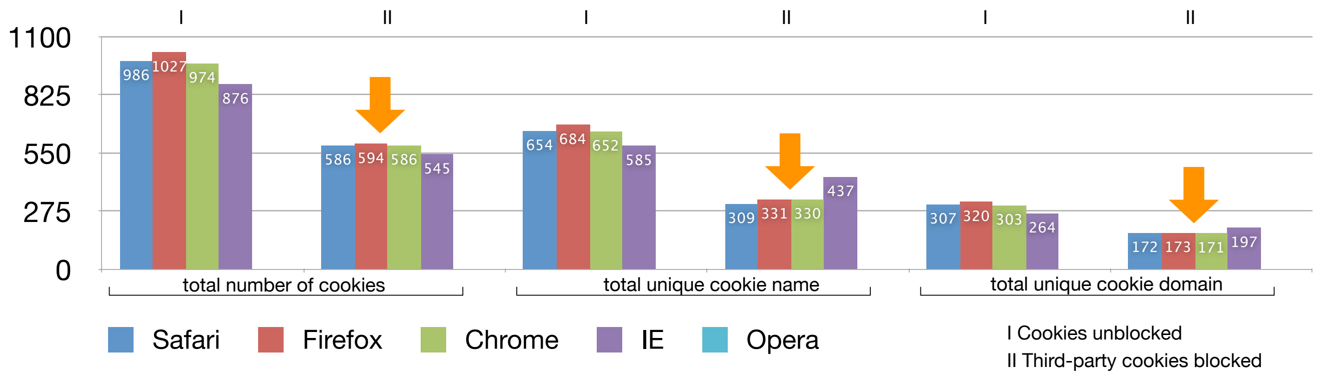


Figure 4 Top five browsers top 100 websites cookie analysis.

V. Conclusion

After analyzing our results, we found that in order to avoid being tracked by third-parties, simply blocking third-party cookies is not enough. In Wireshark we were able to see this clearly, as cookies are set in JavaScript on the first party site so the browser picks them up as first party cookies. Cookie sharing through server synchronization is a possible way that third parties use to obtain user activity information. Although this method is undetectable, it is a possibility that we must consider since it is as simple as a regular site sharing user data with a third party advertiser or analytics company. Cookies set in flash (Locally Stored Objects or LSO's) also go undetected by the major browsers and users are forced to delete them by other means. Web bugs and beacons are usually set as small images on sites and they are used to track activity within a site, while collecting simple data such as IP address. For users to completely avoid being tracked, they may want to implement additional plug-ins on their browser such as:

- ***BetterPrivacy:*** Add-on which allows users to delete LSO's (Flash Cookies)
- ***NoScript:*** Allows JavaScript, Java and other executable content to run only from trusted domains.
- ***Ghostery:*** Detects the "invisible" third party trackers, web bugs, pixels, and beacons placed on web pages by ad networks, behavioral data providers, web publishers, and other companies interested in your activity.

Based on these findings, we can conclude that there is a lack of distinction emerging between first and third party cookies, since there are so many new ways to track user's activities on the web. Since the business models of so many companies rely heavily on this data, they must keep their analytics data accurate so that they can stay relevant. Since blocking third-party cookies has begun to skew their data, third-party cookies have become far less effective than in the past, and new methods of tracking have emerged

Users who block third party cookies have a limited success in avoiding third party tracking. In fact 33% of the sites, who issue the most number of cookies, in our visit to the top 100 with cookies unblocked, were actually from different domains. Advertisers and third party trackers make up to 33%

when looking at the Cookie names. Users who wish to avoid web tracking through cookies must also block some first party cookies.

VI. Acknowledgments

This work was supported in part by TRUST (Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: AFOSR (#FA9550-06-1-0244), BT, Cisco, DoCoMo USA Labs, EADS, ESCHER, HP,IBM, iCAST, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec,TCS, Telecom Italia, and United Technologies.

VII Works Cited

1. *HTTP Cookies: Standards, Privacy, and Politics.* **Kristol, David M.** 2, Nov 2001, ACM Transactions on Internet Technology, Vol. 1, pp. 151–198.

2. Managing Cookies (Windows). *microsoft.com.* [Online] [Cited: July 25, 2010.] http://msdn.microsoft.com/en-us/library/aa385326(VS.85).aspx.

3. **Pegoraro, Rob.** - How to Block Tracking Cookies - washingtonpost.com. *www.washingtonpost.com.* [Online] [Cited: July 25, 2010.] http://www.washingtonpost.com/wp-dyn/content/article/2005/07/16/AR2005071600111.html.

4. *How Google Analytics and Conventional Cookie Tracking Techniques Overestimate Unique Visitors.* **Fomitchev, Max I.** Raleigh : s.n., April 26-30, 2010, pp. 1093-1094.

5. **Colin Crook.** Webtrends Advises Sites to Move to First-Party Cookies Based on Four-Fold Increase in Third-Party Cookie Rejection Rates. *webtrends.com.* [Online] http://www.webtrends.com/CookieRejection.

6. First Party Cookie ConfusionMatt Hopkins. *webanalyticmatt.com.* [Online] [Cited: July 21, 2010.] http://www.webanalyticmatt.com/2007/08/01/first-party-cookie-confusion/.

7. Browser Information. *W3Schools.com.* [Online] [Cited: July 27, 2010.] http://www.w3schools.com/browsers/default.asp.

8. Quantcast - Audience Measurement, Lookalike Modeling, Audience Buying. *quancast.com.* [Online] [Cited: July 27, 2010.] http://www.quantcast.com/top-sites-1.

9. Opera's handling of cookies - Opera Knowledge Base. *opera.com.* [Online] [Cited: July 27, 2010.] http://www.opera.com/support/kb/view/350/.

10. How to delete cookie files in Internet Explorer. *microsoft.com.* [Online] [Cited: July 20, 2010.] http://support.microsoft.com/kb/278835.

11. Microsoft Windows XP - Undestanding cookies. *microsoft.com.* [Online] [Cited: July 20, 2010.] http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sec_cook.mspx?mfr=true.

12. *An Analysis of Private Browsing Modes In Modern Browsers.* **Aggarwal, Gaurav, Jackson, Collin and Boneh, Dan.** 2010.

13. *Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design.* **Friedman, Batya, Howe, Daniel C and Felten, Edward.** 2002. Proceedings of the 35th Hawaii International Conference on System Sciences.

14. *Understading spyware: Risk and response.* **Ames, Wes.** 5, Los Alamitos : IEEE Computer Society, 2004, IT professional , Vol. 6, pp. 25-29.

15. *How to make personalized web browing simple, secure, and anonymous.* **Gabber, Eran, et al.** Murray Hill : Springer, Berlin, ALLEMAGNE, February 24-28, 1997, Lecture notes in computer science.

16. *Cleaning Up After Cookies Version 1.0.* **Mckinley, Katherin.** San Francisco : s.n., December 31, 2008.

17. *On Hit Inflation Techniques and Detection in Streams of Web Advertising.* **Metwally, Ahmed, Agrawal, Divyakant and Abbadi, Amr El.** 2007. 27th International Conference on Distributed Computing Systems (ICDCS'07).

18. *Cookies and Web browser design: toward realizing informed consent online.* **Millett, Lynette I, Friedman, Batya and Felten, Edward.** Washington : ACM, 2001. Proceedings of the SIGCHI conference on Human factors in computing systems. pp. 46-52.

19. *WSKE: Web Server Key Enabled Cookies.* **Masone, Chris, Baek, Kwang-Hyun and Smith, Sean.** s.l. : Springer Berlin / Heidelberg, 2007, Lecture Notes in Computer Science, Vol. 4886.

20. *Automatic Cookie Usage Setting with CookiePicker.* **Yue, Chaun, Xie, Mengjun and Wang, Haining.** 2007, 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07).

21. *Doppelganger: Better browser privacy without the bother.* **Shankar, Umesh and Karlof, Chris.** New York : s.n., 2006. ACM conference on computer and communication security . pp. 154-167.

22. **Soltani, Ashkan, et al.** Flash Cookies and Privacy. August 10, 2009.

23. BetterPrivacy :: Add-ons for Firefox. *addons.mozilla.org.* [Online] [Cited: July 26, 2010.] https://addons.mozilla.org/en-US/firefox/addon/6623/.

24. NoScript :: Add-ons for Firefox. *addons.mozilla.org.* [Online] [Cited: July 22, 2010.] https://addons.mozilla.org/en-US/firefox/addon/722/.

25. Ghostery :: Add-ons for Firefox. *addons.mozilla.org.* [Online] [Cited: July 18, 2010.] https://addons.mozilla.org/en-US/firefox/addon/9609/.

Cookie counting data

The information that proceeds is broken up by browser and the tables are separated by our cookie counting method. The goal is show the numerical difference between third-party cookies unblocked vs. third-party cookies blocked. We collected this data by running a custom script tailored to each browser, and then sorted the data in descending order.

Safari

Third-Party Cookies Unblocked			
Unique Cookie Domain		Unique Cookie Name	
Domain Name	Occurrences	Cookie Name	Occurrences
.insightexpressai.com	23	__qca	40
.pubmatic.com	22	__utma	39
.rubiconproject.com	16	__utmb	39
.revsci.net	13	__utmz	39
.whitepages.com	11	s_vi	25
.ask.com	10	TRUE	23
.casalemedia.com	10	s_pers	10
.people.com	10	rsi_segs	9
.photobucket.com	10	uid	8
.rad.msn.com	10	ACOOKIE	7
.bestbuy.com	9	__qseg	7
.fetchback.com	9	GUID	6
.metacafe.com	9	OAX	6
.microsoft.com	9	WT_FPC	6
.netflix.com	9	ak-mobile-detected	6
.adbrite.com	8	AA002	5
.ads.pointroll.com	8	mbox	5
.att.com	8	v1st	5
.cnet.com	8	BX	4
.zedo.com	8	MUID	4

Third-Party Cookies Unblocked			
Unique Cookie Domain		Unique Cookie Name	
Domain Name	Occurrences	Cookie Name	Occurrences
.whitepages.com	11	__utma	40
.ask.com	10	__utmb	40
.people.com	10	__utmz	40
.photobucket.com	10	__qca	38
.rad.msn.com	10	TRUE	19
.yellowpages.com	10	s_vi	19
.bestbuy.com	9	s_pers	10
.metacafe.com	9	rsi_segs	9
.microsoft.com	9	__qseg	7
.netflix.com	9	WT_FPC	6
.att.com	8	ACOOKIE	5
.cnet.com	8	mbox	5
.candystand.com	7	NGUserID	4
.evite.com	7	s_nr	4
.examiner.com	7	v1st	4
.go.com	7	CFID	3
.huffingtonpost.com	7	CFTOKEN	3
.ign.com	7	GUID	3
.pandora.com	7	MUID	3
.reference.com	7	OAX	3

Firefox

Third-Party Cookies Unblocked			
Unique Cookie Domain		Unique Cookie Name	
Domain Name	Occurrences	Cookie Name	Occurrences
.rubiconproject.com	22	__qca	43
.pubmatic.com	20	__utmz	42
.insightexpressai.com	15	__utma	42
.revsci.net	14	__utmb	42
.photobucket.com	11	s_vi	26
.whitepages.com	11	s_pers	10
.washingtonpost.com	11	rsi_segs	9
.people.com	10	uid	8
.ask.com	10	ACOOKIE	7
.yellowpages.com	10	__qseg	7
.rad.msn.com	10	ak-mobile-detected	6
.fetchback.com	9	GUID	6
ad.yieldmanager.com	9	WT_FPC	6
.huffingtonpost.com	9	OAX	6
.bestbuy.com	9	OAID	6
.netflix.com	9	__g_u	6
.microsoft.com	9	AA002	5
.casalemedia.com	9	v1st	5
.metacafe.com	8	mbox	5
.zedo.com	8	MUID	5

Third-Party Cookies Unblocked			
Unique Cookie Domain		Unique Cookie Name	
Domain Name	Occurrences	Cookie Name	Occurrences
.photobucket.com	11	__utmz	40
.whitepages.com	11	__utma	40
.washingtonpost.com	11	__utmb	40
.people.com	10	__qca	37
.ask.com	10	s_vi	19
.yellowpages.com	10	s_pers	10
.rad.msn.com	10	rsi_segs	8
.metacafe.com	9	__qseg	7
.huffingtonpost.com	9	WT_FPC	6
.bestbuy.com	9	__g_u	6
.netflix.com	9	ACOOKIE	5
.microsoft.com	9	mbox	5
.cnet.com	8	__utmv	4
.att.com	8	v1st	4
.examiner.com	7	s_nr	4
.pandora.com	7	NGUserID	4
.ign.com	7	OAX	3
.go.com	7	CFTOKEN	3
.dailymotion.com	7	CFID	3
.wunderground.com	7	ak-mobile-detected	3

Chrome

Third-Party Cookies Unblocked			
Unique Cookie Domain		Unique Cookie Name	
Domain Name	Occurrences	Cookie Name	Occurrences
.netflix.com	9	ACOOKIE	5
.microsoft.com	9	mbox	5
.cnet.com	8	__utmv	4
.att.com	8	v1st	4
.examiner.com	7	s_nr	4
.pandora.com	7	NGUserID	4
.ign.com	7	OAX	3
.go.com	7	CFTOKEN	3
.dailymotion.com	7	CFID	3
.wunderground.com	7	ak-mobile-detected	3
.netflix.com	9	ACOOKIE	5
.microsoft.com	9	mbox	5
.cnet.com	8	__utmv	4
.att.com	8	v1st	4
.examiner.com	7	s_nr	4
.pandora.com	7	NGUserID	4
.ign.com	7	OAX	3
.go.com	7	CFTOKEN	3
.dailymotion.com	7	CFID	3
.wunderground.com	7	ak-mobile-detected	3

Third-Party Cookies Unblocked			
Unique Cookie Domain		Unique Cookie Name	
Domain Name	Occurrences	Cookie Name	Occurrences
.netflix.com	9	ACOOKIE	5
.microsoft.com	9	mbox	5
.cnet.com	8	__utmv	4
.att.com	8	v1st	4
.examiner.com	7	s_nr	4
.pandora.com	7	NGUserID	4
.ign.com	7	OAX	3
.go.com	7	CFTOKEN	3
.dailymotion.com	7	CFID	3
.wunderground.com	7	ak-mobile-detected	3
.netflix.com	9	ACOOKIE	5
.microsoft.com	9	mbox	5
.cnet.com	8	__utmv	4
.att.com	8	v1st	4
.examiner.com	7	s_nr	4
.pandora.com	7	NGUserID	4
.ign.com	7	OAX	3
.go.com	7	CFTOKEN	3
.dailymotion.com	7	CFID	3
.wunderground.com	7	ak-mobile-detected	3

Internet Explorer

Medium Privacy Setting			
Unique Cookie Domain		Unique Cookie Name	
Domain Name	Occurrences	Cookie Name	Occurrences
interclick.com/	3	vrid	2
webmd.com/	2	gs	1
gigya.com/	1	BizoID	1
www.microsoft.com/	2	scg	1
causes.com/	4	wlidperf	1
ad.wsod.com/	2	PRID	1
openxadmin.netdna.com/	1	AUDid	1
apple.com/	2	bcookie	1
ads.pubmatic.com/	1	gc	1
merriam-webster.com/	4	aud	1
alvenda.com/	2	KRTBCOOKIE_57	1
bbc.co.uk/	3	PRgo	1
legolas-media.com/	3	segments	1
pronto.com/	5	_csoot	1
www.msn.com/	1	pubfreq_16238_11042_1030962336	1
undertone.com/	1	p_first_entry	1
crwdcntrl.net/	1	Apache	1
teracent.net/	2	tg	1
break.com/	5	dsavip	1
www.mtv.com/	1	pubfreq_22621	1

High Privacy Setting			
Unique Cookie Domain		Unique Cookie Name	
Domain Name	Occurrences	Cookie Name	Occurrences
interclick.com/	4	gs	1
gigya.com/	1	BizoID	1
causes.com/	4	scg	1
ad.wsod.com/	2	wlidperf	1
mathtag.com/	1	PRID	1
apple.com/	1	bcookie	1
ads.pubmatic.com/	1	gc	1
content.yieldmanager.com/ak/	1	aud	1
bluestreak.com/	1	KRTBCOOKIE_57	1
cnet.com/	8	PRgo	1
legolas-media.com/	3	segments	1
undertone.com/	1	p_first_entry	1
www.burstnet.com/	1	Apache	1
edgeadx.net/	1	tg	1
suresafe1.adsovo.com/	1	dsavip	1
cookie.monster.com/	1	pubfreq_22621	1
ebayrtm.com/rtm	1	AA002	4
opt.fimserve.com/	4	DMEXP	1
photobucket.com/	2	_UR	1
doubleclick.net/	1	O65121	1