Scott A. Kamber (*pro hac vice*)
skamber@kamberlaw.com
David A. Stampley (*pro hac vice*)
dstampley@kamberlaw.com
KamberLaw, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 202-6364

Interim Class Counsel

David C. Parisi (SBN 162248)
dcparisi@parisihavens.com
Suzanne Havens Beckman (SBN 188814)
shavens@parisihavens.com
Parisi & Havens LLP
15233 Valleyheart Drive
Sherman Oaks, California 91403
Telephone: (818) 990-1299
Facsimile: (818) 501-7852

Attorneys for Plaintiffs
Additional counsel listed on signature page

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

In Re QUANTCAST ADVERTISING COOKIE LITIGATION In Re CLEARSPRING FLASH COOKIE LITIGATION	No. 2:10-CV-05484-GW-JCG No. 2:10-CV-05948-GW-JCG [Assigned to the Hon. George H. Wu] **JOINT SUBMISSION OF SUPPLEMENTAL INFORMATION REGARDING PLAINTIFFS' MOTION FOR PRELIMINARY APPROVAL OF CLASS ACTION SETTLEMENT** Date: January 13, 2011 Location: Courtroom 10 312 North Spring Street Los Angeles, CA 90012 Time: 8:30 a.m.

This Joint Supplemental Information Submission Regarding Plaintiff's Motion for Preliminary Approval of Class Action Settlement is submitted in response to the Court's December 16, 2010 request that the parties furnish additional information about the technology at issue in the litigation and how and when defendants Quantcast and Clearspring used that technology and the data derived from it.

How Do Third Parties "See" Web Users?[1]

Each time an Internet user directs his or her browser to a website by entering a web page address (*i.e.*, its universal resource locator, or URL, and path information), or navigates from one page to another by clicking on a hypertext link, here is what actually happens: the user's browsing software (browser) transmits hypertext transfer protocol (HTTP) commands to request the page from the server where the web page resides.[2] These commands include information about the user's browser and the user's IP (Internet Protocol) address (essentially, the user's return address). The server responds by transmitting the contents of a document that contains the web page expressed in hypertext markup language (HTML). The user's browser processes the HTML code, which tells the browser how to display the web page on the user's computer. (To view the actual HTML code, a user can click *View* > *Source* option on the browser menu bar.)

Often, a web page's HTML code will include commands to download additional files. For example, the HTML code for the text of a news article may be stored in one file on the news organization's server (*e.g.*, *http://www.news-org.com/topstory*) while the photos that accompany the article may be stored in

[1] For purposes of this document, this section includes descriptions of typical and representative, but not the sole, technologies used in web communications.

[2] The global standard for HTTP communications was defined in "RFC 2616, Hypertext Transfer Protocol—HTTP/1.1," Fielding, *et al.*, Internet Engineering Task Force (IETF), June 1999, available at http://www.ietf.org/rfc/rfc2616.txt.pdf (last accessed January 1, 2011).

other files (*e.g.*, *http://www.newsorg.com/photolib/topstory-pic1* and *http://www.-newsorg.com/photolib/topstory-pic2*). Thus, a user's single request to view a web page may trigger multiple requests to download content from multiple servers without further action or even awareness on the user's part. Some of this embedded web page content, such as advertisements, may come from third-party servers, *i.e.*, from domains controlled by parties other than the website the user chose to visit.

Some embedded images are invisible to the user. For example, when a website wants to use a third-party service to monitor traffic levels on a web page, the website may embed third-party images that display nothing at all, but permit the third party to monitor user activity. These images, known as "web beacons" (the term preferred by the advertising industry), "pixel tags," "clear GIFs," or "web bugs," are so small the user cannot see them but, just like a web page statement to display an advertisement, they cause the user's browser to communicate with the third party's server. In the process, the user's browser automatically sends the third party information that includes details about the user's browser and Internet address, making the user "visible" to the third party.

What is an HTTP cookie?

Although the communications process of downloading web content makes a user somewhat visible to the party hosting that content, it does not necessarily make the user recognizable. For example, the user's IP "return" address allows a third party to send the user's browser an advertisement to be embedded in a web page display, but the IP address does not reliably allow the advertiser to recognize that it is serving an ad to the same user the next day or even a few minutes later.

This is because, in the most basic user-server communications on the web, each communication is "stateless." That is, even though the user may have a sense of being "connected to" a website, no continuous connection exists. The user has merely downloaded one or more documents that are displayed on the user's com-

puter screen. When the user clicks on a hypertext link on the web page, the user initiates a download request that starts from scratch, without any history or context from the page the user was just viewing, such as whether the user was viewing an online shopping cart and is now ready to pay for the items in the cart. Without any way to maintain a continuous state of user-to-server communications, the web cannot support complex transactions—such as online shopping—that require a succession of related web page displays and user responses.

To avoid this disconnection from page view to page view or session to session, HTTP includes a mechanism by which a website can affix identifying information to a user's browser, to "recognize" the user and "remember" the last exchange in the communication between user and server. That mechanism is an HTTP cookie. A cookie is a small string of text transmitted to and from a user's computer in a communication between a server group and a particular instance of browser client software.[3] A cookie may contain whatever information the website obtains from or attaches to the user, such as a zip code entered by the user for viewing the local weather each time the user visits the website, a username the user selected for interactions with the website, or a unique identifier the website operator assigns to the user.

Cookies transmitted from a website are automatically stored by the browser on the user's computer. Each cookie is a separate file. On each new page view, the website operator can read, update, or replace the cookie. One website operator can

[3] The global standard for HTTP cookies was initially defined in "RFC 2965, HTTP State Management Mechanism," Kristol and Montulli, Internet Engineering Task Force, Oct. 7, 2000, available at http://www.ietf.org/rfc/rfc2965.txt.pdf (January 3, 2011); *see also*, "RFC 2964, BCP (Best Current Practice) 44, Use of HTTP State Management," Moore and Freed, Internet Engineering Task Force, Oct. 12, 2000, available at http://www.ietf.org/rfc/rfc2964.txt.pdf (last accessed January 3, 2011).

set multiple cookies on a user's computer and, at any point in time, the typical user's computer may contain hundreds or thousands of cookies.[4]

For browsers that operate according to IETF standards, the operator of one website cannot view the contents of another website operator's cookie. However, when a website operator is a third-party advertiser or metrics company, it can set a common cookie that it uses to track a user's activities across the many websites on which it serves ads or gathers traffic data.

By default, commercial browsers, such as Firefox or Internet Explorer, assume a user wants to accept first-party cookies (from the visited website) and third-party cookies (such as those from advertisers and metrics companies). A user who does not want these parties to set cookies can change the default browser setting and block all cookies, although doing so would likely render many websites nonfunctional. A user who does not want to be tracked by third parties can set his or her browser controls to block only third-party cookies (although even this action may affect the functionality of some websites). For example, in Safari, this control is accessed as follows:

> Safari > Preferences > Security > Accept cookies: Only from sites I visit / Block cookies from third parties and advertisers

In addition, a user can delete browser cookies previously stored by third parties to attempt to prevent the third party from associating previously acquired tracking data with the consumer's subsequent web activity. Blocking or deleting can be accomplished "by hand," that is, for specific cookies, or automatically, using tools

[4] For example, a number of U.S. district courts set a cookie called "MENU" that, in at least some instances, contains a single word, such as "slow." In addition, some U.S. courts set cookies named "_utmz" and "_utma" that contain lengthy numeric and alphanumeric codes.

available in or in addition to the browser. Mechanisms to block and delete third-party cookies are generally available to consumers using commercial browsers.

See Exhibit A, attached, for an illustration of third-party data collection on a web page.

What is a "Flash cookie"?

Adobe Flash Player, a popular program originally distributed by Macromedia Corp. and now distributed by Adobe Corporation, is widely used to display videos and games. Flash Player has its own method—called local shared objects, or "LSOs"—of storing bits of data on the computers using the software. For example, many online games run in Adobe Flash Player. If a user seeks to play a game over multiple sessions, Flash stores information about the player's previous session, including where the player left off, in an LSO. Where Flash Player operates on a news or sports website, to use another example, the LSO may contain information about the user's volume choice, screen resolution and other settings, so the user does not need to select those settings on each subsequent visit to the same site. According to Adobe, LSOs were designed to support consumers' ability to experience "rich Internet application" content using the Adobe Flash Player. Letter to FTC, Adobe Systems Inc., Jan. 27, 2010, available at http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf (last accessed Dec. 6, 2010).

Just as with HTTP cookies, Flash Player LSOs can be set to contain unique user identifiers. There are, however, important differences between HTTP cookies and Flash Player LSOs: for example, Flash Player LSOs can be much larger than HTTP cookies (four kilobytes for cookies versus up to 100 kilobytes for LSOs), can contain more complex information, and, by default, do not expire. LSOs also are stored in a different place than HTTP cookies and are not deleted or rejected

when a user instructs his or her browser to delete or not to accept HTTP cookies.[5] In addition, as mentioned above, HTTP cookies are designed so that one website operator cannot read cookies set by another website operator whereas LSOs permit "cross-domain" access. Website operators using LSOs can override the requirement to maintain encrypted communications that a user establishes with a secure (HTTPS) website. Finally, HTTP cookies are essentially vendor-independent; the manner in which they operate is governed by global standards and by usage conventions shared by all commercially available browsers. LSOs are subject to Adobe Corporations implementation of Flash Player software.

How Do Quantcast and Clearspring Use Cookies and LSOs?

A study entitled "Flash Cookies and Privacy" was published in August 2009 by the University of California, Berkeley and is annexed hereto as Exhibit B (the "Berkeley Study"). Plaintiffs' Consolidated Amended Complaint refers extensively to the Berkeley Study. Quantcast and Clearspring concur with the material findings of the Berkeley Study specifically to Quantcast and Clearspring and to the extent it reported observations relating collectively to third-party metrics and advertising companies that include Quantcast and Clearspring,

Quantcast and Clearspring further offer the following description of their current uses of cookies and LSOs.

When a user visits a website (call it "Widget.com"), the user may receive a cookie from Widget.com itself, but also may receive third party cookies placed by advertisers on or vendors to the Widget.com website. In the case of defendant Quantcast, for example, the operators of the Widget.com website may wish to determine how many unique (vs. repeat) visitors view the website during a given period—a service Quantcast provides. To provide this service, Quantcast places a

[5] Adobe offers a tool for managing LSOs. This tool resides on Adobe's servers and is proprietary to Adobe. *See* http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html (last accessed January 3, 2011).

very simple cookie on the user's computer containing only a randomly-generated number and the time of day. In the Widget.com example, when the user commands his or her computer to load the Widget.com web page, Widget.com's HTTP code would cause the user's computer also to query Quantcast. If the user's computer already had a Quantcast number cookie stored on it, the request the user's computer sends to Quantcast would contain a copy of that previously-set Quantcast cookie, allowing Quantcast to determine if the user is a new visitor or one who has visited the Widget.com site before. If the user has no extant Quantcast cookie, Quantcast will count the user as a new visitor, and send one.

Quantcast collects no personally-identifiable information in this process. All it does is assign an anonymous user a random number. But—and this is the key to Quantcast's service—when that user visits either Widget.com again, or another website serviced by Quantcast, Quantcast can tell that he or she is the *same* anonymous user who visited Widget.com previously.

Clearspring uses cookies for similar anonymous purposes. Clearspring provides a service that allows website publishers to include online "buttons" on their websites, which visitors to the websites can click on to quickly share website content to social networks like Facebook and other online destinations. At certain times, Clearspring has utilized HTTP cookies and LSOs to anonymously track basic information about users' interactions with the websites that use its tools. For example, when a user visits a website that uses Clearspring's technology, Clearspring places a cookie on the user's computer with a unique computer-generated number so that it can count the number of unique users to the particular web page (in other words, if that same user visits the webpage again, Clearspring will know not to count that user again because it will know from the unique identifier on the cookie that the user has previously visited the website). Like Quantcast, Clearspring's use of cookies and LSOs has at all times been limited to these anonymous types of web analytics and Clearspring has never used cookies or LSOs to track

personally identifiable information. Moreover, both Clearspring and Quantcast no longer store information from LSOs at all in any of their services.

The sorts of anonymous information maintained in cookies are useful for a number of reasons. One important reason is that Internet advertising (and thus the economic viability of the Internet) depends on the ability to measure *unique* visitors to a website. Advertisers need to know how many *different* people their ads will reach for a given cost. It is far more valuable to an advertiser to have multiple people view its ad once than to have a single user view it multiple times. As noted above, however, the Internet is inherently stateless. Thus, if one's browser is constantly refreshing (for example) a news site or the progress of a sporting event, the same user's computer may query the same website hundreds of times in an hour. Absent a cookie of the type placed by Quantcast and Clearspring, the website operator would not know if those requests were coming from the same user or different users. This type of cookie also allows website operators to better understand what various content on its site the same user chooses to visit, how long the same user spends on the site, etc.[6]

As companies that provide advertising-related services, Quantcast and Clearspring generate information about the same users' visits to multiple websites with which those networks have relationships. They can determine, for example, that an anonymous user assigned number "12345678" visited Widget.com and then WidgetReviews.com (assuming both those sites have relationships with the same network). Like any other website operator, however, Quantcast and Clearspring can see and update only the cookies they themselves placed; they cannot

[6] At best, this method can provide only a fairly accurate picture of the number of unique visitors to a site. If a user deletes his or her cookies from one browsing session to the next, he or she will be assigned a new random number upon the next visit to the website, and be considered a second unique visitor, rather than the return visitor he or she actually is. Various methodologies exist to correct for this effect, but none are perfect.

see the contents of the first-party cookies placed by the website the user is visiting. Thus, even if the user identifies himself or herself by name to the first-party website, Quantcast and Clearspring do not learn that name or any other information passed from the user to the first-party website.

Simply knowing that the same user visited multiple websites, however, as Quantcast and Clearspring do, facilitates "Online Behavioral Advertising" (or "OBA"). Without collecting personally-identifiable information or knowing a user's identity, but by placing a unique identifier cookie, it is possible to determine that the visitor to a particular news site today visited a particular car company's website yesterday and a travel company's website the day before. Knowing this information, the news site can show the user an ad for a new car or for a travel service, and can seek a higher price for the placement of that ad, because the consumer viewing the ad has a demonstrated likelihood to find the ad useful. This kind of targeted advertising helps advertisers, enables millions of website operators to provide deep, broad, and useful content free of charge to the consumer, and, for that reason, is seen by many as pro-consumer.[7] Although no one likes advertising in the abstract, much of the Internet is free only because of advertising, and if people must view ads, many may prefer to see one for something they might want rather than for goods or services they don't want. Neither Clearspring nor Quantcast has ever delivered OBA based on LSOs, and Clearspring only began offering advertising-related service in December 2009 using a platform that utilizes only HTTP cookies, which are not at issue in this litigation.

[7] Quantcast and Clearspring also provide methods for consumers to "opt out" of receiving any OBA. They accomplish this by placing what is known as an "opt out" cookie on the user's computer, which instructs Defendants not to serve targeted ads to that user. Quantcast is a member of the Network Advertising Initiative ("NAI") and complies with the NAI's opt-out procedures.

Quantcast and Clearspring's Former Use of LSOs

Quantcast and Clearspring further make the following representations about their former uses of cookies and LSOs.

The differences between LSOs and HTTP cookies gave rise to the since-discarded practice underlying this dispute. As noted, users must employ different tools to manage or delete HTTP cookies and LSOs. As a result, (again using Quantcast's past system as an example) a Quantcast-placed LSO and a Quantcast-placed HTTP cookie on the same computer, which should contain the same unique, anonymous identifier, might not. If a user deleted his or her HTTP cookies, the next HTTP request to Quantcast would cause the creation of a new unique identifier. In an attempt not to count the same user as multiple unique visitors to the same sites, Quantcast formerly utilized a synchronization process. The process looked at the various cookies, and, if they did not match, found the oldest value, and set the others to the same value, bringing them back into synch.

Clearspring's use of LSOs was similar. When Clearspring stored an LSO on a computer, it also stored a back-up HTTP cookie at the same time. Both cookies contained the same anonymous user ID number and were used for the same anonymous purpose as described above. If a user deleted the HTTP cookie (but not the LSO) and then later accessed a web page using Clearspring's technology, Clearspring's servers would detect that there was an LSO but no HTTP cookie associated with the computer. Clearspring's systems would then place a new HTTP cookie that would adopt the same user ID as the existing LSO. This unique user ID is the *only* information that was restored in this process and the *only* consequence to the user was that Clearspring would then use the LSO and back-up HTTP cookie for the same anonymous analytics as described above (put simply, no personally identifiable information was impacted by the use of LSO). Again, Clearspring and Quantcast no longer use LSOs even for this limited purpose.

As researchers discovered and publicized in the Berkeley Study last August, this synchronization process had a side effect. Viewed from the user's perspective, the Berkeley Study portrayed, and Plaintiffs in this action contend that the effect of synchronizing HTTP cookies and LSOs in circumstances where a user had deleted his or her HTTP cookie was to regenerate or "respawn" this information, which the user had deleted, and to do so without the user's express consent.

The Berkeley Study researchers published their findings on August 10, 2009. By August 12, 2009, Quantcast had modified its systems to cease "respawning." Since then, if a user deletes his or her Quantcast-placed HTTP cookies, they stay deleted, and any newly-placed cookies would contain a new identifier unrelated to the value contained in the user's LSOs or prior HTTP cookies.

Quantcast and Clearspring both have represented that they had no intention to return to the prior practice and, under the proposed settlement, they will be enjoined from doing so. They also will agree to provide consistent and reliable disclosure of other uses of Flash LSOs. Those provisions are set out in detail in the settlement agreement and proposed orders. Briefly summarized, they (*i*) ban entirely the use of LSOs to respawn HTTP cookies; (*ii*) prohibit the use of LSOs "as an alternative method to HTTP cookies for storing information about a user's web browsing history, unrelated to the delivery of content through the Flash Player or the performance of the Flash Player in delivering such content, without adequate disclosure"; (*iii*) prohibit the use of LSOs to "otherwise counteract any computer user's decision to either prevent the use of or to delete previously created HTTP cookies"; and, (*iv*) require Defendants to advocate that the relevant trade associations adopt such provisions as model rules for the use of LSOs by all of their members. The parties believe that these provisions will provide important privacy protections to all Internet users, and will assure that the issues raised by the previous use of LSOs to respawn cookies will not recur.

Other Defendants and Settlement Participants

The Berkeley Study (Exhibit B hereto) reported on substantially similar practices of a number of other third-party metrics and advertising companies. Some of these entities are named in other cases pending before this Court and other U.S. District Courts. The representations herein relate to Quantcast and Clearspring

The defendants in this matter other than Quantcast and Clearspring are arm's-length customers of Quantcast and/or Clearspring ("Customer Defendants"). The consolidated complaint alleges class members had contact with Quantcast and/or Clearspring when class members accessed the Customer Defendants' websites and web content.

The Customer Defendants, on their own behalf and on behalf of their corporate parents and affiliates, have represented to Quantcast and Clearspring that the Customer Defendants were unaware that LSOs were being used to store information regarding consumers who accessed their websites and web content. Quantcast and Clearspring do not dispute that representation and, to the extent of their knowledge, information, and belief, adopt and incorporate it here.

In the settlement agreement before the Court, certain participants are referred to as "Undertaking Parties." The Undertaking Parties consist of Customer Defendants and certain of the Customers Defendants' corporate parents or affiliates who have agreed to undertake the obligations imposed by the settlement agreement. The remedial value of the injunctive relief agreed to by the Undertaking Parties is generally applicable to their relationships with any of the third-party metrics and advertising companies identified in the Berkeley Report and benefits any classes of consumers that might have been affected by the conduct of those companies. Because the scope of injunctive relief agreed to by the Undertaking Parties encompasses relationships they had with Quantcast and Clearspring, plus any relationships they may have had with other third-party metrics and advertising

companies, the proposed settlement would provide the Undertaking Parties with a release from claims involving Quantcast and Clearspring as well as the other third-party metrics and advertising companies.

Should the Court have questions about the relevant technologies not addressed in this submission or in the attached Berkeley Report, the parties will be prepared to address those questions at the hearing currently scheduled for January 13, 2011.

DATED: January 7, 2011

Respectfully submitted,

KAMBERLAW, LLC

s/David A. Stampley

Scott A. Kamber
David A. Stampley
KamberLaw, LLC
100 Wall Street, 23rd Floor
New York, New York 10005

Interim Class Counsel

COOLEY LLP

s/Michael Rhodes

Whitty Somvichian
101 California Street, 5th Floor
San Francisco, California 94111
Attorneys for Defendant

Clearspring Technologies, Inc.

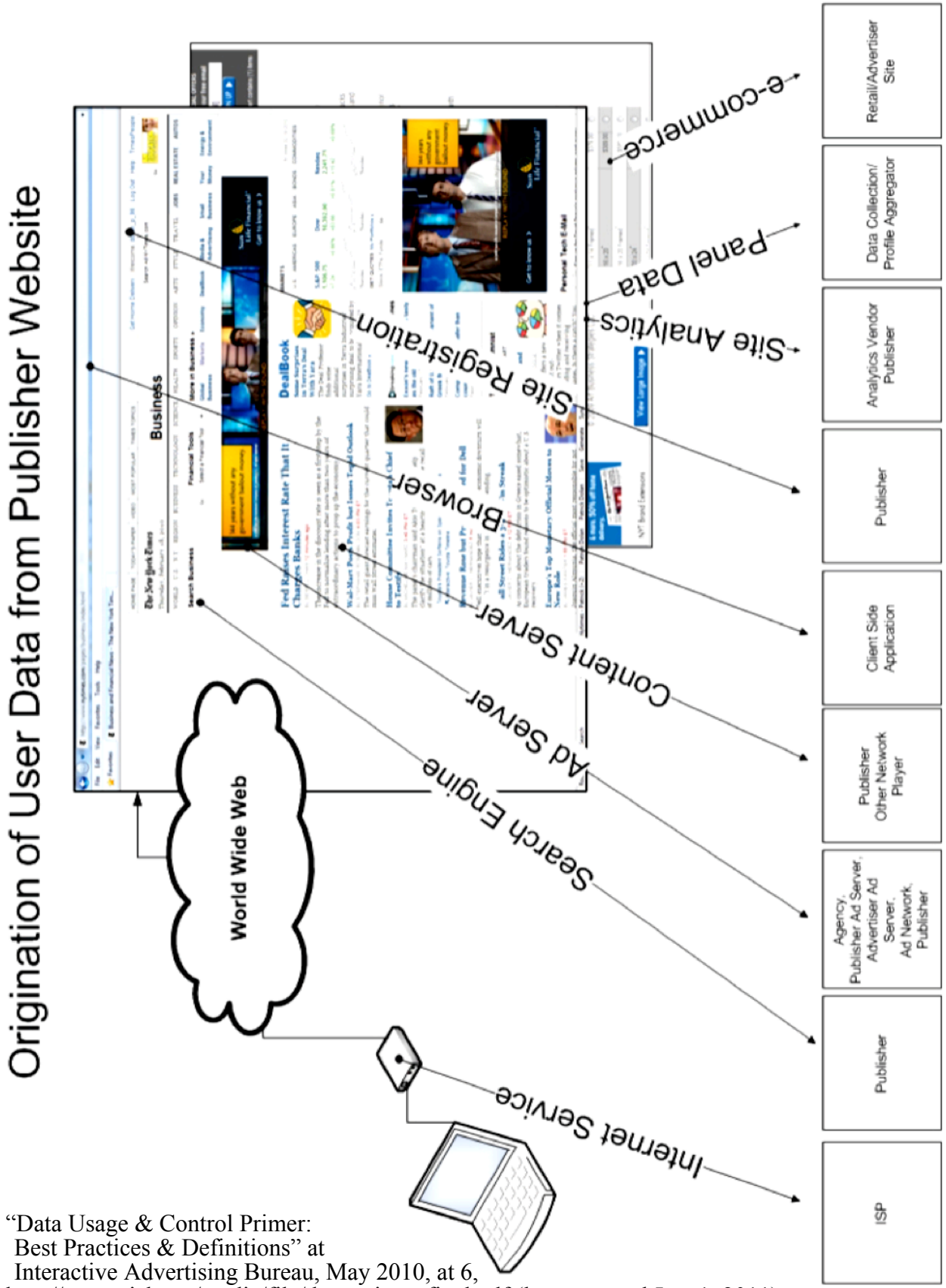
DURIE TANGRI LLP

s/Michael H. Page

Michael H. Page
217 Leidesdorff Street
San Francisco, California 94111

Attorneys for Defendant Quantcast Corp.

EXHIBIT A



"Data Usage & Control Primer: Best Practices & Definitions" at Interactive Advertising Bureau, May 2010, at 6, http:// www.iab.net/media/file/data-primer-final.pdf (last accessed Jan. 1, 2011).

EXHIBIT B

Flash Cookies and Privacy

Ashkan Soltani[A], Shannon Canty[B][1], Quentin Mayo[B][2], Lauren Thomas[B][3] & Chris Jay Hoofnagle[C]
School of Information[A]
Summer Undergraduate Program in Engineering Research at Berkeley (SUPERB) 2009[B]
UC Berkeley School of Law[C]
University of California, Berkeley
Berkeley, USA
correspondence to: choofnagle@law.berkeley.edu

Abstract—**This is a pilot study of the use of "Flash cookies" by popular websites. We find that more than 50% of the sites in our sample are using Flash cookies to store information about the user. Some are using it to "respawn" or re-instantiate HTTP cookies deleted by the user. Flash cookies often share the same values as HTTP cookies, and are even used on government websites to assign unique values to users. Privacy policies rarely disclose the presence of Flash cookies, and user controls for effectuating privacy preferences are lacking.**

Privacy, tracking, flash, cookies, local stored objects, usability, online advertising, behavioral targeting, self-help

I. INTRODUCTION

Advertisers are increasingly concerned about unique tracking of users online.[4] Several studies have found that over 30% of users delete first party HTTP cookies once a month, thus leading to overestimation of the number of true unique visitors to websites, and attendant overpayment for advertising impressions.[4]

Mindful of this problem, online advertising companies have attempted to increase the reliability of tracking methods. In 2005, United Virtualities (UV), an online advertising company, exclaimed, "All advertisers, websites and networks use [HTTP] cookies for targeted advertising, but cookies are under attack."[5] The company announced that it had, "developed a backup ID system for cookies set by web sites, ad networks and advertisers, but increasingly deleted by users. UV's 'Persistent Identification Element' (PIE) is tagged to the user's browser, providing each with a unique ID just like traditional cookie coding. However, PIEs cannot be deleted by any commercially available anti-spyware, mal-ware, or adware removal program. They will even function at the default security setting for Internet Explorer."[5] (Since 2005, a Firefox plugin called "BetterPrivacy", and more recently, a shareware program called "Glary Utilities Pro" can assist users in deleting Flash cookies.)

United Virtualities' PIE leveraged a feature in Adobe's Flash MX: the "local shared object,"[6] also known as the "flash cookie." Flash cookies offer several advantages that lead to more persistence than standard HTTP cookies. Flash cookies can contain up to 100KB of information by default (HTTP cookies only store 4KB).[7] Flash cookies do not have expiration dates by default, whereas HTTP cookies expire at the end of a session unless programmed to live longer by the domain setting the cookie. Flash cookies are stored in a different location than HTTP cookies,[7] thus users may not know what files to delete in order to eliminate them. Additionally, they are stored so that different browsers and stand-alone Flash widgets installed on a given computer access the same persistent Flash cookies. Flash cookies are not controlled by the browser. Thus erasing HTTP cookies, clearing history, erasing the cache, or choosing a delete private data option within the browser does not affect Flash cookies. Even the 'Private Browsing' mode recently added to most browsers such as Internet Explorer 8 and Firefox 3 still allows Flash cookies to operate fully and track the user. These differences make Flash cookies a more resilient technology for tracking than HTTP cookies, and creates an area for uncertainty for user privacy control.

It is important to differentiate between the varying uses of Flash cookies. These files (and any local storage in general) provides the benefit of allowing a given application to 'save state' on the users computer and provide better functionality to the user. Examples of such could be storing the volume level of a Flash video or caching a music file for better performance over an unreliable network connection. These uses are different than using Flash cookies as secondary, redundant unique identifiers that enable advertisers to circumvent user preferences and self-help.

With rising concern over "behavioral advertising," the US Congress and federal regulators are considering new rules to address online consumer privacy. A key focus surrounds users' ability to avoid tracking, but the privacy implications of Flash cookies has not entered the discourse.

Additionally, any consumer protection debate will include discourse on self-help. Thus, consumers' ability to be aware of and control unwanted tracking will be a key part of the legislative debate.

To inform this debate, we surveyed the top 100 websites to determine which were using Flash cookies, and explored the privacy implications. We examined these sites' privacy policies to see whether they discussed Flash cookies.

We also studied the privacy settings provided by Adobe for Flash cookies, in an effort to better understand the practical effects of using self-help to control Flash cookies. Because some sites rely so heavily on the use of Flash content, users may encounter functionality difficulties as a result of enabling these privacy settings.

We found that Flash cookies are a popular mechanism for storing data on the top 100 sites. From a privacy perspective, this is problematic, because in addition to storing user settings, many sites stored the same values in both HTTP and Flash cookies, usually with telling variable names indicating they were user ids or computer guids

(globally unique identifiers). We found that top 100 websites are using Flash cookies to "respawn,"[1] or recreate deleted HTTP cookies. This means that privacy-sensitive consumers who "toss" their HTTP cookies to prevent tracking or remain anonymous are still being uniquely identified online by advertising companies. Few websites disclose their use of Flash in privacy policies, and many companies using Flash are privacy certified by TRUSTe.

II. FLASH COOKIES

Some exposition on Adobe's system for managing Flash cookies is necessary here.

Flash data is stored in a different folder on different computing platforms. For instance, on an Apple, Flash local shared objects (labeled .sol) are stored at:

/users/[username]/Library/Preferences/Macromedia/Flash Player/

On a Windows computer, they are stored at:

\Documents and Settings\[username]\Application Data\Macromedia \Flash Player

Several subdirectories may reside at that location: "#SharedObjects" contains the actual Flash cookies and subdirectories under "Macromedia.com" contains persistent global and domain-specific settings for how the Flash player operates. As such, there will be a subdirectory for each Flash-enabled domain a user visits under the "Macromedia.com" settings folder. This has privacy implications that will be visited in section IV(F) below.

A Flash cookie can be set when a websites embeds first party or third party Flash content on a page. For instance, a website may include animated Flash banner advertisements served by a company that leases the advertising space or they may embed a hidden SWF used solely to provide metrics on the user. Thus, merely visiting some websites (without actually clicking on an advertisement or video) can cause Flash data from a third party advertiser to be stored on the user's computer, often unbeknownst to the user.

III. METHODS

We analyzed HTTP and Flash cookies from the top 100 domains ranked by QuantCast results of July 1, 2009. The data for this survey were captured on July 27, 2009.

We also analyzed six additional government websites: CDC.gov, DATA.gov, DHS.gov, IRS.gov, NASA.gov, and Whitehouse.gov. We took care not to leave the top-level domain when analyzing these sites. That is, the URL always displayed the domain to be analyzed during our browsing session.

A. Potential for Tracking

We used Mozilla Firefox 3.5 (release June 30, 2009) and Windows XP Professional Version 2002 Service Pack 3 for capturing data from the top 100 websites. To avoid contamination from different domains visited, we created a small program to handle the process of deleting all data stored between sessions since Firefox's "Clear Private Data" tool does not remove stored Flash objects.

Each session consisted of starting on a Firefox about:blank page with clean data directories. We then navigated directly to the site in question (by entering the domain name into the browser's navigation bar) and mimicked a 'typical' users session on that site for approximately 10 pages. For example, on a video site, we would search for content and browse videos. On a shopping site, we would add items to our shopping cart. We did not create accounts or login for any of the sites tested. As a result, we had to 'deep link' directly into specific user pages for sites such as Facebook.com or Myspace.com since typically these sites do not easily allow unauthenticated browsing.

We used SoThink SWF Catcher, a Firefox plugin which identifies all SWF files present on a webpage, to capture the Flash content encountered throughout the user session. We also quit the browser after each session and ran a program to capture the resulting persistent data such as HTTP cookies, Flash objects, and the Firefox cache.

Because of the dynamic nature of websites and online advertising, any given survey may produce different advertisements and correspondingly different Flash data from varied advertising networks. Thus, our snapshot of HTTP and Flash cookies may differ from another user's experience. However we feel that this provides reasonable sample for an initial study.

1) Respawning Deleted HTTP cookies

To manually test for HTTP cookie respawning, we used Safari 4.0.1 in a clean state (no HTTP or Flash cookies as well as no items in the browser cache) to visit a top 100 site. After browsing on the site and HTTP and Flash cookies are acquired, we deleted all HTTP cookies, cleared the cache, and restarted the browser, but did not modify the Flash cookies. We then visited the same site and noted the values of HTTP cookies set and whether they matched the Flash cookies set in the previous session.

B. Implications of Manipulating User Controls

We tested usability to explore how a hypothetical privacy-sensitive user's experience would differ if his/her settings were changed to restrict Flash cookies. The test was performed using Mozilla Firefox with the BetterPrivacy 1.29 add-on installed. BetterPrivacy provides an easy-to-use interface to review, protect or delete Flash cookies. Flash player settings are controlled via a webpage on Adobe.com's website called the Adobe Flash Player: Settings Manager[8].

The user navigated to each of the top 100 websites and took notes of any pop-ups, broken content, or any other abnormalities experienced while browsing the site. Each session began with clearing all non-Adobe Flash Player shared object files (i.e. those not under the Macromedia.com folder), navigating to the site in question, and then mimicking a 'typical' user's session. Caution was taken not to navigate away from the domain of the site being tested. After each session, BetterPrivacy was checked for the appearance of any Flash cookies that may have been accumulated while browsing the site.

[1] We use the popular gamer word "respawn" to describe the recreation of a HTTP cookie after its affirmative removal by the user.

We attempted to identify changes in user-experience after restricting the ability for third party Flash objects from being stored on a user's computer (first party objects were still allowed). This option is enabled by: navigating to the Adobe Flash Player Settings Manager, locating the 'Global Storage Settings' option panel, then deselecting the option that reads, "Allow third party flash content to store data on your computer."

IV. Results and Discussion

A. Presence of Flash and HTTP Cookies

We encountered Flash cookies on 54 of the top 100 sites. These 54 sites set a total of 157 Flash shared objects files yielding a total of 281 individual Flash cookies.

Ninety-eight of the top 100 sites set HTTP cookies (only wikipedia and wikimedia.org lacked HTTP cookies in our tests). These 98 sites set a total of 3,602 HTTP cookies.

Thirty-one of these sites carried a TRUSTe Privacy Seal. Of these 31, 14 were employing Flash cookies.

Thus, both HTTP and Flash cookies are a popular mechanism on top 100 websites.

B. Common Flash Cookie Variable Names

We attempted to infer the potential use of Flash cookies via examining the actual variable names for each cookie. Often, developers will use the term 'uid' or 'userid' to refer to a unique identifier whereas 'volume' could suggest volume settings for a music or video player. Below is a table of the most frequently occurring names in our sample.

Cookie Name	Frequency
volume	21
userid	20
user	14
id	8
lts	6
_tpf	6
_fpf	6
uid	5
perf	5
computerguid	5

The most frequently occurring Flash cookie outside of those used in the Flash Player system directory was 'volume'. Given the dominance of Flash video on the web, it is reasonable to expect that volume settings would be a commonly occurring use of Flash cookies. However, it is surprising with which the prominence of Flash cookies such as 'userid, user, and id', which were found to store unique identifiers which could be used to track the user, were found. It's also worth mentioning that '_tpf' and '_fpf' were found to also contain unique identifiers which were also found to contain overlapping values as the ones found in HTML cookies for 'uid' or 'userid'.

C. Shared Values Between HTTP and Flash Cookies

Of the top 100 websites, 31 had at least one overlap between a HTTP and Flash cookie. For instance, a website might have an HTTP cookie labeled "uid" with a long value such as 4a7082eb-775d6-d440f-dbf25. There were 41 such matches on these 31 sites.

Most Flash cookies with matching values were served by third-party advertising networks. That is, upon a visit to a top 100 website, a third party advertising network would set both a third party HTTP cookie and a third party Flash cookie. Our tests revealed 37 matching HTTP and Flash values from the following advertisers: ClearSpring (8), Iesnare (1), InterClick (4), ScanScout (2), SpecificClick (14), QuantCast (6), VideoEgg (1), and Vizu (1).

In 4 cases, the following first-party domains HTTP cookies matched Flash cookie values: Sears, Lowe's, AOL, and Hulu.

D. Flash Cookie Respawning

Shared values between HTTP and Flash cookies raises the issue of whether websites and tracking networks are using Flash cookies to accomplish redundant unique user tracking. That is, storing the same values in both the Flash and HTTP cookie would give a site the opportunity to backup HTTP cookies if the user deleted them.

We found that taking the privacy-conscious step of deleting HTTP cookies to prevent unique tracking could be circumvented through "respawning" (See Figures 1-3). The Flash cookie value would be rewritten in the standard HTTP cookie value, thus subverting the user's attempt to prevent tracking.

We found HTTP cookie respawning on several sites.

On About.com, a SpecificClick Flash cookie respawned a deleted SpecificClick HTTP cookie. Similarly, on Hulu.com, a QuantCast Flash cookie respawned a deleted QuantCast HTTP cookie.

We also found HTTP cookie respawning across domains. For instance, a third-party ClearSpring Flash cookie respawned a matching Answers.com HTTP cookie. ClearSpring also respawned HTTP cookies served directly by Aol.com and Mapquest.com. InterClick respawned a HTTP cookie served by Reference.com

E. Interaction with NAI Opt-Out

"The NAI (Network Advertising Initiative) is a cooperative of online marketing and analytics companies committed to building consumer awareness and establishing responsible business and data management practices and standards."[9] Since some of the sites using Flash cookies also belong to the NAI, we tested the interaction of Flash cookies with the NAI opt-out cookie.

We found that persistent Flash cookies were still used when the NAI opt-out cookie for QuantCast was set. Upon deletion of cookies, the Flash cookie still allowed a respawn of the QuantCast HTML cookie (see Figures 4-7). It did not respawn the opt-out cookie. Thus, user tracking is still present after individuals opt out.

F. Presence of Flash Settings Files

Adobe Flash settings files (those in the Macromedia.com folder) were set by Flash player in visits to 89 of the top 100 sites. A total of 201 settings files were present among these 89 sites. This is relevant, because each settings file is stored in its own directory, labeled by domain. This creates a type of history file parallel to the one created by the browser. However, the Flash history is not deleted when browser controls are used to erase information about sites previously visited. This means that users may falsely believe that they have fully cleared their history when using the standard browser tools.

G. Privacy Policies

We searched the privacy policies of the top 100 sites, looking for terms such as "Flash," "PIE," or "LSO." Only 4 mentioned the use of Flash as a tracking mechanism.

Given the different storage characteristics of Flash cookies, without disclosure of Flash cookies in a privacy policy, it is unclear how the average user would even know of the technology. This would make privacy self-help impossible except for sophisticated users.

H. Government Sites

The Obama Administration is considering whether to change policy concerning the use of HTTP cookies on government websites. Currently, government officials require a "compelling need" to use persistent HTTP cookies, and must disclose their use in a privacy policy.

In light of this we arbitrarily chose six government websites to determine whether Flash was being used to assign unique values to visitors. Of the 6 government sites we tested, 3 had Flash cookies. Three were set by whitehouse.gov, one of which was labeled, "userId." Five of these sites used persistent HTTP cookies.

Whitehouse.gov disclosed the presence of a tracking technology in its privacy policy, but the policy does not specify that Flash cookies are present, nor does it provide any information on how to disable Flash cookies.[10]

I. User Experience

Since users generally do not know about Flash cookies, it stands to reason that users lack knowledge to properly manage them. In comments to the New York Times, Emmy Huang of Adobe said, "It is accurate to say that the privacy settings people make with regards to their browser activities are not immediately reflected in Flash Player. Still, privacy choices people make for their browsers aren't more difficult to do in Flash Player, and deleting cookies recorded by Flash Player isn't a more difficult process than deleting browser cookies. However, it is a different process and people may not know it is available."[11]

A separate issue arises with user controls: if a privacy sensitive individual knows about them and employs them, will they still be able to use the internet normally?

When disabling third party content, we found that 84 of the sites had no functionality issues after third-party Flash content was disabled. Sixteen sites stored some type of Flash data.

Ten sites did not function optimally with third party context storage disabled. Nine of these 10 sites would not display Flash content. One site displayed an advertisement intermittently that never stabilized.

V. Conclusion

Flash cookies are a popular mechanism for storing data on top 100 websites. Some top 100 websites are circumventing user deletion of HTTP cookies by respawning them using Flash cookies with identical values. Even when a user obtains a NAI opt-out cookie, Flash cookies are employed for unique user tracking. These experiences are not consonant with user expectations of private browsing and deleting cookies. Users are limited in self-help, because anti-tracking tools effective against this technique are not widespread, and presence of Flash cookies is rarely disclosed in privacy policies.

A tighter integration between browser tools and Flash cookies could empower users to engage in privacy self-help, by blocking Flash cookies. But, to make browser tools effective, users need some warning that Flash cookies are present. Disclosures about their presence, the types of uses employed, and information about controls, are necessary first steps to addressing the privacy implications of Flash cookies.

Acknowledgments

This work was supported in 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, ESCHER, HP, IBM, iCAST, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec, Telecom Italia, and United Technologies. We are grateful for the opportunities offered by the Summer Undergraduate Program in Engineering Research at Berkeley (SUPERB), and to its program leaders, Dr. Kristen Gates, Dr. Sheila M. Humphreys, and Beatriz Lopez-Flores.

References

[1] Shannon Canty is a senior at Clemson University majoring in bioengineering.

[2] Quentin Mayo is a senior at Jacksonville State University majoring in computer science.

[3] Lauren Thomas is a senior at Louisiana State University majoring in industrial engineering.

[4] M. Abraham, C. Meierhoefer, and & A. Lipsman, "The Impact of Cookie Deletion on the Accuracy of Site-Server and Ad-Server Metrics: An Empirical Comscore Study," 2007, available at http://www.comscore.com/Press_Events/Presentations_Whitepapers/2007/Cookie_Deletion_Whitepaper.

[5] United Virtualities, "United Virtualities develops ID backup to cookies, Browser-Based 'Persistent Identification Element' will also restore erased cookie, Mar. 31, 2005, available at http://www.unitedvirtualities.com/UV-Pressrelease03-31-05.htm.

[6] Antone Gonslaves, "Company bypasses cookie-deleting consumers, March 31, 2005, available at http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=160400801.

[7] J. Lott, D. Schall, and K. Peters, Actionscript 3.0 Cookbook, O'Reilly, 2006, p. 410.

[8] Adobe, Flash Settings Manager, available at http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html

[9] NAI, About the NAI, available at http://www.networkadvertising.org/about/.

[10] The White House, Our Online Privacy Policy, n.d., available at http://www.whitehouse.gov/privacy/

[11] Stone, Brad. "Adobe's Flash and Apple's Safari Fail a Privacy Test." Technology - Bits Blog – NYTimes.com. 30 Dec. 2008. 23 June 2009 http://bits.blogs.nytimes.com/2008/12/30/adobes-flash-and-apples-safari-fail-a-privacy-test

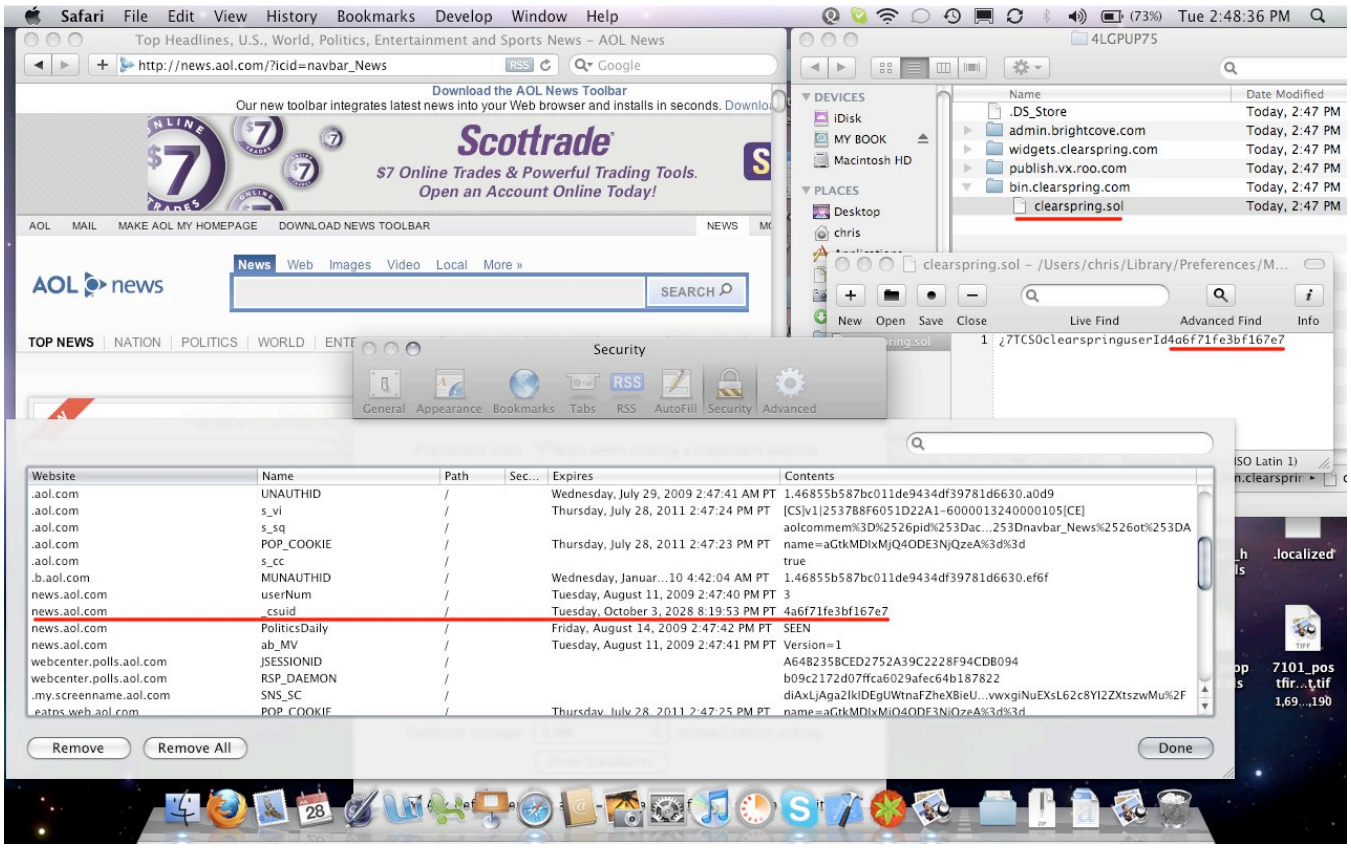


Figure 1: A matching Flash and HTTP cookie is set by AOL.com and ClearSpring.

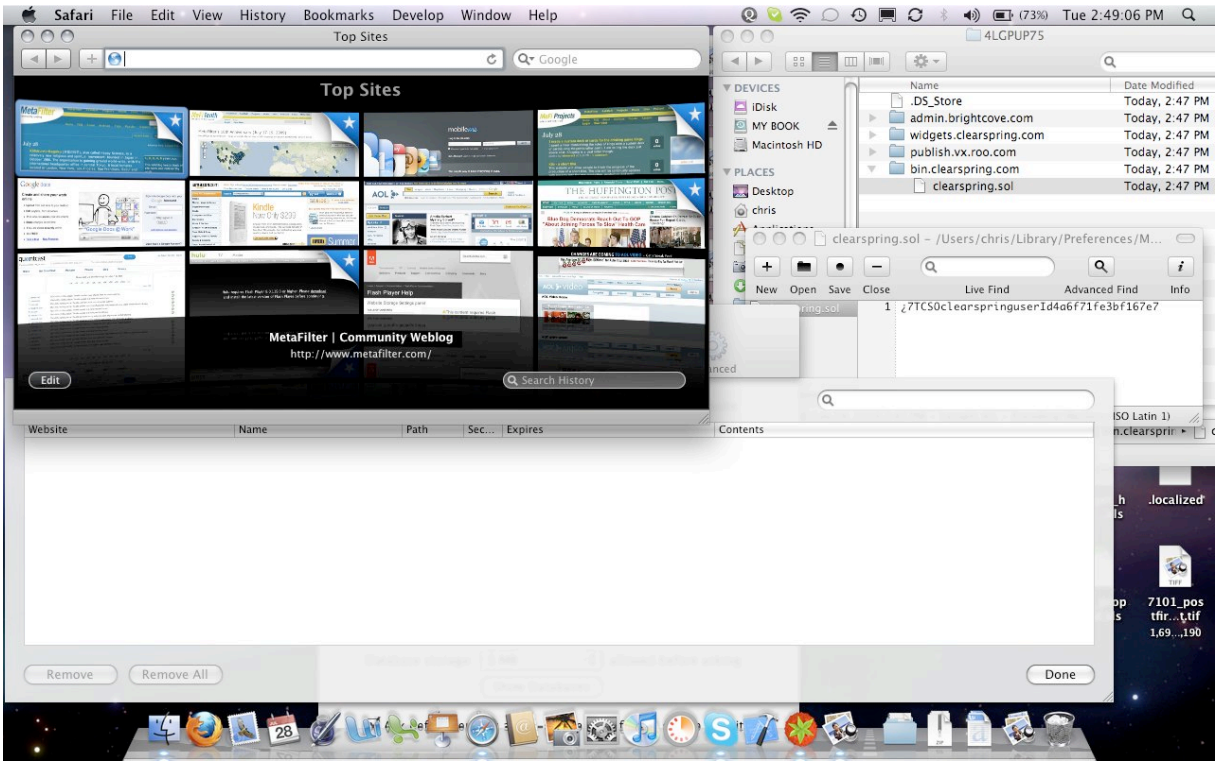


Figure 2: The researcher deleted HTTP cookies and cleared the cache, leaving the Flash cookies unaltered

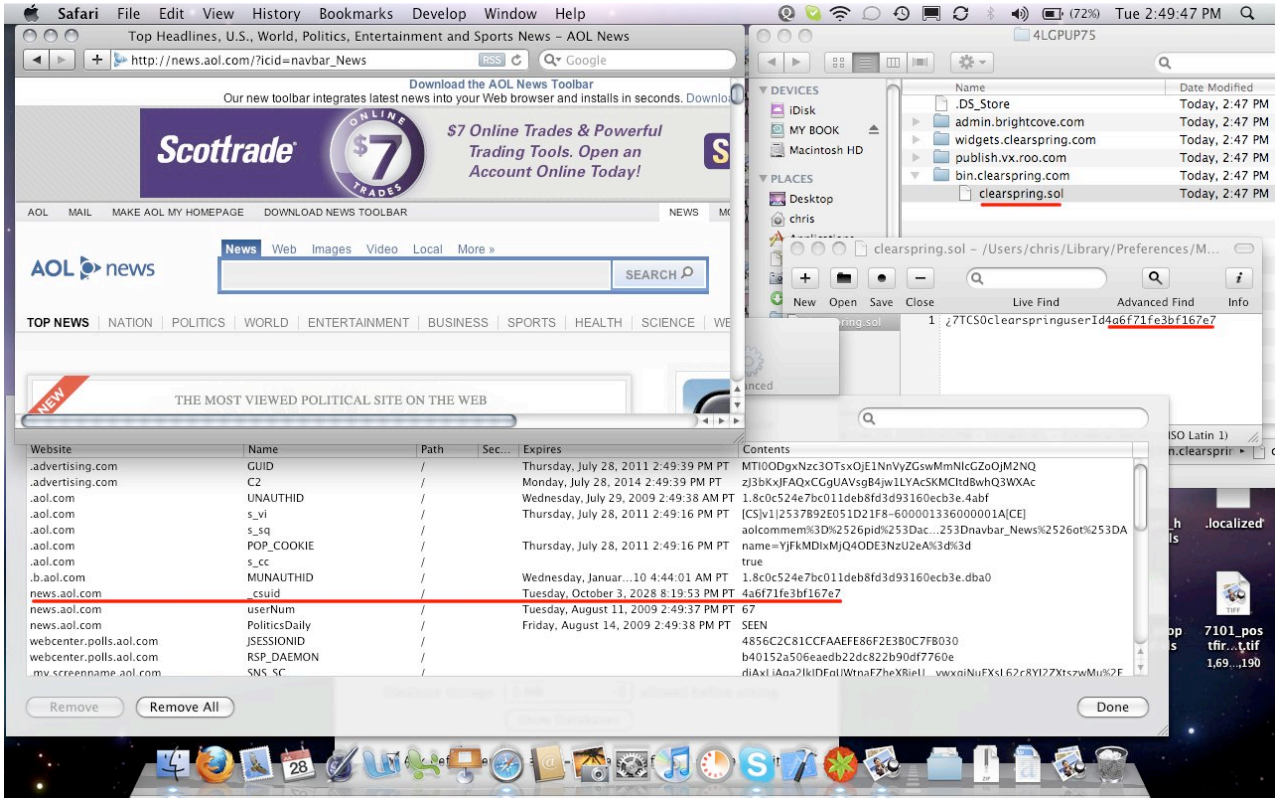


Figure 3: Upon revisiting AOL.com, a new HTTP cookie is set with the same value before HTTP cookies were deleted

Quantcast

If you were not opted out successfuly, you may try again by clicking here or you can go directly to Quantcast's Web site.

Figure 4: Researcher obtains opt-out cookie from QuantCast

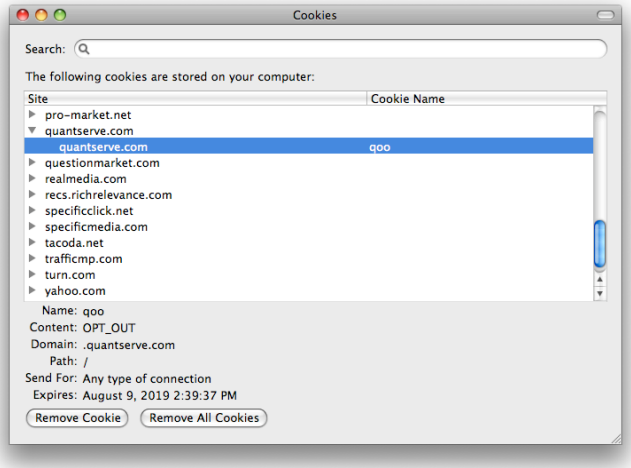


Figure 5: QuantCast opt-out cookie is retained

Figure 6: Even after opting out, a Flash tracking cookie is present

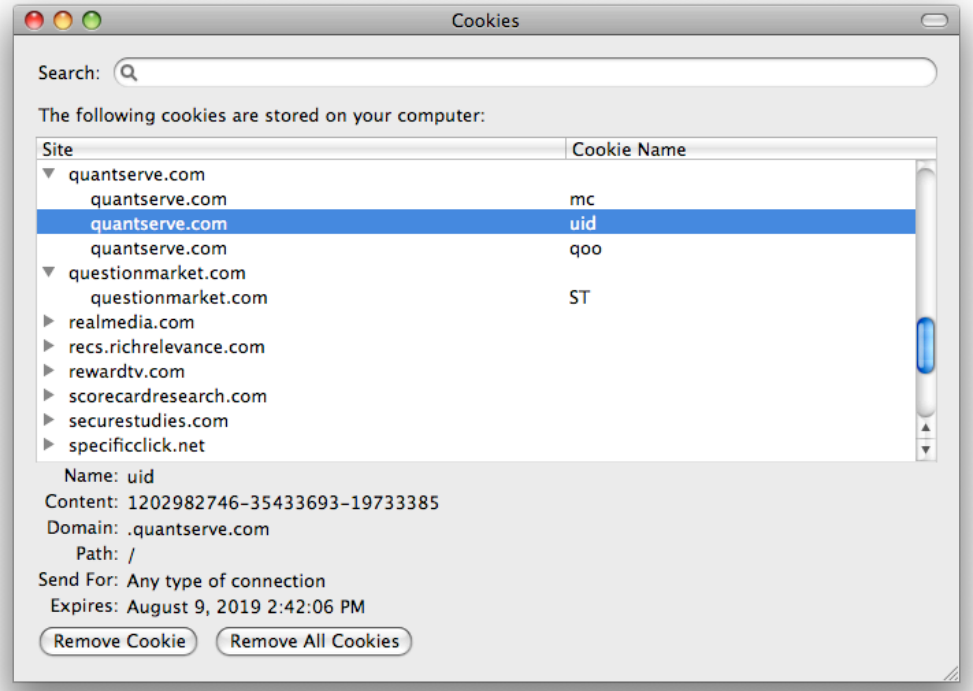


Figure 7: Flash tracking cookie matches Quantserve uid cookie