

21874972185632987492187401299
5091298-048123895683274509238
32985639847927830918-39-30=149
938409218497398584593355 2167
87497218563298749218740113449

BPA Whitepaper: **The Use of Flash Objects in Visitor Tracking:** **Brilliant Idea or Risky Business?**

Executive Summary

Web site owners and operators frequently express concerns about the accuracy of data collected and reported during the audience measurement process. Historically browser cookies have been used to improve the accuracy of measurement, but privacy concerns, anti-spyware applications, and in some instances governmental regulation limits the utility of this approach. In response, some site operators are turning to a widely deployed but poorly understood strategy -- the use of Flash Local Shared Objects (LSO), as a harder-to-remove alternative to cookies. In this paper we outline the reasons for the use of LSOs and our view of the risks LSOs create from a consumer awareness and privacy perspective.

Our recommendations are to be thoughtful and careful about how Flash objects are used in audience measurement. If they are to be used at all, business owners need to ensure that:

- A) they are not used to over-ride consumer preferences;
- B) consumers are made aware of their use via normal channels (e.g., privacy policy);
- C) consumers are given an easy way to opt-out of their use as a tracking mechanism.

While these recommendations may be somewhat controversial within the audience measurement community, we firmly believe that the line between using Flash to improve accuracy and using Flash in conflict with consumer preferences is black and white.

Introduction

One of the great challenges facing the web site operators, media buyers, and audience measurement specialists is how to accurately identify and track individual people over time to better estimate audience size, better target, and better optimize the overall customer experience online. While it may not be immediately obvious, the ability to track individuals is quite difficult for a variety of reasons including:

- People use different computers at different times of the day (work, home)
- People have different computers in the home (office, family, personal)
- People use different devices to connect to the Internet (computer, phone)
- Multiple people might share devices (family computer, public terminals)
- People actively work to block and prevent audience tracking technology

In general there are two strategies for counting the largely anonymous audiences most sites attract: panel-based services and the use of so-called “browser cookies.” While the former is a widely accepted practice, in reality panels are typically quite small relative to the online population often making their ability to provide audience data for smaller sites limited, especially in “at work” situations where the deployment of panel-measurement technology is often disallowed. The latter approach -- the use of small text files called “cookies” placed on individual computers and devices -- is far more popular and is more or less ubiquitous within connected channels.

The Use of Browser Cookies

A cookie is, in its purest form, a small text file written directly to the hard drive of a connected computer or device. Cookies are used for a variety of things:

- Cookies give web sites the ability to remember preferences
- Cookies can be used to remember credentials

- Cookies can be used to uniquely identify web browsers such as Internet Explorer, Firefox, and Apple Safari

It is this last use of cookies—uniquely identifying web browsers—that is commonly used as a proxy for counting unique individuals, even though in practice cookies are a poor proxy at best. Cookies are a poor proxy because of the aforementioned difficulty associated with tracking individuals on the Internet: any one person using a home computer, a work computer, and a connected mobile device would log three cookies and be counted three times, clearly a case of over-counting.

The use of cookies can be improved as an identifier for individuals in some cases—on sites requiring authentication or other secure environments—but in general the assumption that any number of “counted cookies” is directly related to the number of people generating those cookies is fallacious. In fact, in 2008 the Internet Advertising Bureau (IAB) published a set of definitions for use in audience reach measurement that explicitly differentiated “Unique Cookies”, “Unique Browsers”, “Unique Devices” and “Unique Users”¹.

Unfortunately, by their own admission, few companies have started to apply the IAB guidelines and most persist in conflating “cookies” and “users,” thereby choosing ease over accuracy, despite repeated claims of the importance of accuracy in measurement². Perhaps more unfortunate is the reliance companies have on cookie-based measurement, despite longstanding and well-supported observation that cookies are far from reliable as a *tracking* mechanism^{3,4}. While more research into the phenomenon of cookie deletion needs to occur, the reality is that in many cases cookies are a poor approximation of audience size.

1 http://www.iab.net/iab_products_and_industry_services/508676/guidelines/audiencemeasurement

2 <http://www.analyticsevolution.com/2009/07/forrester-wave-just-facts-please.html>

3 <http://www.webmediabrands.com/corporate/releases/05.03.14-newjupresearch.html>

4 http://www.comscore.com/Press_Events/Press_Releases/2007/04/comScore_Cookie_Deletion_Report

Why People Delete Cookies

Hard data is difficult to come by regarding why people remove cookies, Anecdotal evidence suggests that viewing of less-socially acceptable content (gambling, pornography) plays a role. Other studies suggest that consumers delete cookies because they simply do not want to be tracked, period. Walt Mossberg of the *Wall Street Journal* perhaps best expressed anti-cookie sentiment when he commented in 2005, “To me, tracking cookies clearly meet the obvious definition of spyware.⁵” While some people noted that Mr. Mossberg’s comments are reactionary, he is not alone in his opinion, and data suggests that many consumers still regularly delete their browser cookies. Regardless of the reason, consumers actively and willingly deleting their browser cookies continue to erode the efficacy of this tool as a mechanism for accurately tracking audiences and individuals. While unfortunate, this behavior is an expression of personal preference and, in *Web Analytics Demystified*’s opinion, one that should be respected.

When is a Cookie Not a Cookie? When it is a Local Shared Object

As evidence for the fragility of browser cookies increasing through the early part of this decade, some smart engineers went looking for an alternative, seeking another place to identify information that was less likely to be deleted. They found what they were looking for in Adobe Flash’s Local Shared Objects. According to the Wikipedia:

“A Local Shared Object (LSO) is a collection of cookie-like data stored as a file on a user’s computer. LSOs are used by all versions of Adobe Flash Player and Version 6 and above of Macromedia’s now-obsolete Flash MX Player. LSOs contain cookie-like data stored by individual web sites or domains.”

The Local Shared Objects solved the cookie removal problem because, again from Wikipedia, “With the default settings, Adobe Flash Player does not seek the user’s permission to store LSO files on the hard disk.” Given the ubiquity of Adobe’s Flash player, estimated to be installed in 98 percent of all personal

5 http://online.wsj.com/article_email/SB112129842537185221-1BjflNilaV4opynalCHa6mFm4.html

computers and an increasing number of smart phones and mobile devices, Flash Local Shared Objects appear to be a perfect solution—a local storage mechanism that doesn’t bother to ask permission prior to being set.

The Use of Flash LSOs in Audience Measurement

While there are many appropriate and beneficial uses for Flash Local Shared Objects—for example, remembering volume settings in a Flash-based media player or keeping other application-specific preferences—it is increasingly clear that in some cases the data contained in the Flash object are being used for consumer tracking purposes.

In their 2009 report *Flash Cookies and Privacy*⁶, Ashkan Soltani and his co-authors at the University of California reported that 31 percent of the Quantcast Top 100 web sites appeared to be using Flash LSO to store some type of unique user identifier. Flash Local Shared Objects are also commonly used in video-tracking services such as those provided by Omniture, Nielsen NetRatings, and Visible Measures among others, and are potentially used on cell phones thanks to increasing deployment of the Flash platform on mobile browsing platforms⁷⁸. What’s more, some sites are clearly using Flash LSO to “reset” browser cookies—storing a tracking value in the Flash Object and then using that value to continually refresh and restore the browser cookie—effectively over-riding any consumer preference to not be tracked over time. The following diagram explains very basically what happens when Flash is used to reset browser cookies:

While this “reset” (or “respawning” using Soltani’s language) was primarily observed in third-party advertising technology, and at least one company has stopped using LSOs to reset browser cookies⁹, Web Analytics Demystified is aware of non-advertising instances of the same resetting happening on consumer-facing web sites. Respawning confers another advantage to more technical users in that it apparently allows cookie values to be copied between

- 6 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862
- 7 http://www.adobe.com/devnet/devices/articles/persistent_data.html
- 8 <http://mashable.com/2009/11/17/adobe-flash-player-10-1/>
- 9 <http://www.wired.com/epicenter/2009/08/flash-cookie-researchers-spark-quantcast-change/>

browser applications (for example, from Internet Explorer to Firefox) given that Flash is likely in both pieces of software.

Web Analytics Demystified fully understands why site developers and audience measurement specialists would want to use Flash LSOs to reset cookies; the aforementioned data regarding cookie deletion and the resulting impact on audience counting creates a clear need for better audience tracking. The ability to “reset” a unique identifier in the aftermath of a cookie deletion event is vital from an accuracy standpoint and has the potential to improve the quality of targeting, tracking, and visitor segmentation that has become fundamental in online audience research. However, in reality Flash does little to mitigate over-counting due to the use of multiple computers.

Even without resetting browser cookie values, storing a unique identifier in a place less likely to be removed or deleted can impart the ability to calculate the cookie deletion rate for a given site -- a very useful and often hard to come by measurement. A good analyst armed with a trustworthy count of “unique visitors” which can be compared with the number of “unique cookies” recorded is well on his or her way toward understanding cookie deletion behavior, especially if the Flash LSO value is made available to a moderately robust analytics package for further exploration.

In Web Analytics Demystified’s opinion, the problem is not that Flash LSOs are being used; the problem is that they are being used in most cases without transparency and consumer controls, and in a way likely to be labeled “deceptive” by some.

Transparency and the use of Flash Local Shared Objects

According to Soltani et al. more than half of the sites they reviewed were using Flash LSO to store information about site users. Regarding consumer awareness and controls for Flash LSO, the authors commented:

“Privacy policies rarely disclose the presence of Flash cookies, and user controls for effectuating privacy preferences are lacking.”

More colloquially, on the subject of Flash LSO the Wikipedia notes:

“LSOs can be used by web sites to collect information on how people navigate those web sites even if people believe they’ve restricted the data collection. There is relatively little public awareness of LSOs, and they can usually not be deleted by the cookie privacy controls in a web browser. This may lead a web user to believe a computer is cleared from

tracking objects, when it is not.”

Unfortunately disclosure about the use of Flash LSO for tracking purposes is rare on the Internet today. Soltani et al. reviewed the privacy policies of the Quantcast Top 100 sites and only found mention of Flash LSO four times. Our own search failed to find any immediately relevant sites and privacy policies¹⁰. Given the lack of disclosure and transparency found, Web Analytics Demystified agrees strongly with Soltani’s statement regarding “Flash cookies” (their term for Local Shared Objects):

“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 about the technology. This would make privacy self-help impossible except for sophisticated users.”

Regarding communication and trust, one of the most widely known champions is the TRUSTe organization¹¹. While Soltani reports that 31 of the Top 100 sites they looked at carried the TRUSTe Privacy Seal, they also found that 14 were using Flash LSO (but did not report whether LSOs were being used for tracking or other purposes.)

Web Analytics Demystified contacted TRUSTe and found them to be both candid and helpful regarding the use of Flash LSO. According to Joanne Furtsch, TRUSTe’s Policy and Product Architect, the company is currently recommending that clients using Flash LSO add the following to their privacy statements:

“We use Local Shared Objects, also known as Flash cookies, to store some of your preferences or to display content based upon what you view on our site to personalize your visit. Third Parties, with whom we partner to provide certain features on our site or to display advertising based upon your Web browsing activity, use Flash cookies to collect and store information.

Flash cookies are different from browser cookies because of the amount of, type of, and how data is stored. Cookie management tools provided by your browser will not remove Flash cookies. To learn how to manage privacy and storage settings for Flash cookies click here: http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_

10 <http://www.google.com/search?q=%22privacy+policy%22+AND+%22Flash%22>

11 <http://www.truste.com>

manager.html”

This statement is an excellent step in the right direction, although the only site using this kind of disclosure on the Internet today (based on a Google search for the phrase “We use Local Shared Objects, also known as Flash cookies”) is Bunnyhero Labs of Toronto, Ontario (Canada)¹² and they were using LSO to remember settings, not track visitors.

All of the above becomes even more important from a global perspective when one considers recent legislation in Europe designed to create an entirely new consumer relationship with browser cookies. In a nutshell, the Council of the European Union (EU) voted in November 2009 to require that European businesses using browser cookies in nearly all capacities, stating that a cookie can be stored on a user’s computer, or accessed from that computer, only if the user “has given his or her consent, having been provided with clear and comprehensive information”¹³.

Clearly there is an opportunity for companies using Flash LSOs to improve the quality of messaging to their site users and consumers in general. Still, making consumers aware of Flash LSO and having them manage the objects at their discretion are two different problems.

Controlling How Flash LSOs are Used

To confirm that Flash LSOs are being used currently, the author used Firefox’s “BetterPrivacy” add-on¹⁴ and was able to discover a staggering number of LSO files (Figure 1) stored on his computer.

12 <http://bunnyherolabs.com/privacyarchive/privacy20070628.php>

13 <http://www.out-law.com/page-10510>

14 <https://addons.mozilla.org/en-US/firefox/addon/6623>

View remove or protect Local Shared Objects stored on your computer:

Folder/Site	LSO File Name	Modified	Status
www.theonion.com	com.quantserve.sol	Tue Aug 11 19:58:07 2009	Not protected
www.theonion.com	theonion.sol	Tue Aug 11 19:57:59 2009	Not protected
www.veoh.com	com.quantserve.sol	Tue Jan 6 22:54:52 2009	Not protected
www.veoh.com	veohUser.sol	Tue Apr 21 08:44:26 2009	Not protected
www.veoh.com	veohVolume.sol	Fri Apr 17 20:01:24 2009	Not protected
www.vw.com	logfile_0.sol	Fri Nov 14 15:06:28 2008	Not protected
www.vw.com	logfile_dir.sol	Fri Nov 14 15:06:28 2008	Not protected
www.vw.com	VWDealerSession.sol	Fri Nov 14 15:06:57 2008	Not protected

Information about the selected Local Shared Object:

FileName: StreamMinerInfo.sol
Folder/Site: illumenix.com
FileSize: 59 bytes
Path: /Users/ericpeterson/Library/Preferences/Macromedia/Flash Player/#SharedObjects/2ZJSH58G/illumenix.com
Modified: Thu Sep 18 14:10:08 2008

Figure 1: Sample of LSO files found on the author’s computer via the “BetterPrivacy” Firefox add-on.

These objects live outside of the browser and outside of Platform for Privacy Preferences (P3P) controls, the primary control over which cookies are set and which are denied. Suffice to say, the author had no idea that these LSOs were present on his computer prior to starting work on this paper.

Flash LSO also appear to be impervious to the “Private Browsing” modes recently deployed by Firefox, Microsoft, and Apple in their browsing platforms, which given the current prevalence of use of the technology more or less obviates the value of “Private Browsing”, leaving a still discoverable trail through any site using Flash LSO for any reason.

Regarding exerting control over Flash LSOs, while Firefox users are able to install the “BetterPrivacy” add-on, other browser users are essentially forced to use Adobe’s Flash Player Settings Manager¹⁵ found on the Adobe/Macromedia web site (Figure 2)

¹⁵ http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html

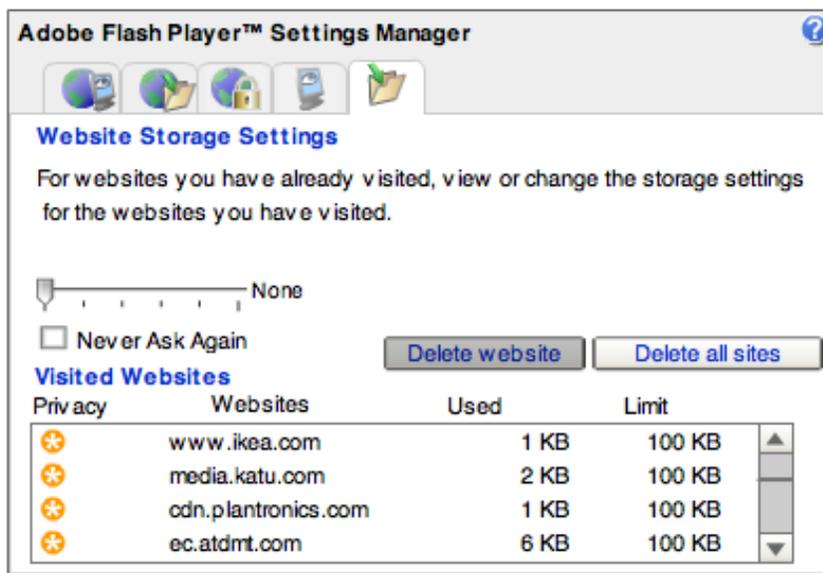


Figure 2: Adobe Flash Player Settings Manager, run via a web page on the Adobe web site.

While certainly functional, the Settings Manager application is far from visible and even less easy to use. On this point, Emmy Huang, Adobe’s product manager for the Flash Player, was quoted in a 2008 article in the *New York Times* as saying:

“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.”

Given that deleting browser cookies can be done directly from within the browsing application itself and is usually clearly labeled as part of a “Security” or “Privacy” setting’s list, not to mention new one-click “Private Browsing” options found in most browsers, the necessity to manage Flash LSOs via an external

web site makes us question the accuracy of Ms. Huang’s statement.

Best Practices for Using Flash LSOs in Audience Measurement

Considering all of the previous information, and given our belief that use of Flash Local Share Objects is unlikely to lessen, Web Analytics Demystified recommends the following best practices to site operators and audience measurement specialists using this technology for tracking purposes:

1. Do not use Flash to reset browser cookies
2. Disclose the use of Local Shared Objects
3. Allow site visitors to disable Local Shared Objects

For sake of clarity, we explore each of these recommendations in the following sections.

Don’t Use Flash to Reset Browser Cookies

From an audience measurement perspective this is certainly the most controversial of our recommendations. It is, however, the recommendation we believe to be most important. Consider:

- Consumer feelings regarding the use of cookies and tracking in general runs “hot” publically, and national governments continually review cookie use policy¹⁶ as a privacy matter;
- There is copious evidence of a distinct subset of Internet users who are adamantly anti-tracking¹⁷;
- Deleting or disabling cookies, at least with the most widespread methodologies, has no impact on the use of Flash Local Shared Objects.¹⁸

With these three points in mind, Web Analytics Demystified believes that sites

16 <http://blog.ostp.gov/2009/07/24/cookiepolicy/>

17 <http://www.blogcatalog.com/discuss/entry/tracking-cookies-suck>

18 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862

and services using Flash to reset and “respawn” browser cookie values in an effort to improve accuracy of tracking and targeting run the risk of being identified as “unconcerned about consumer preferences and privacy” and badly treated in the court of public opinion. Given that Quantcast has already changed their use of Flash cookies¹⁹ and other vendors are moving in the same direction, Web Analytics Demystified believes that other companies using Flash LSOs in this way are likely to be similarly identified and pressured to change their approach. The alternative for those audience measurement specialists wishing to use Flash Local Shared Objects to better understand cookie deletion rates (in an effort to better estimate audience size) is to store a second, unrelated but unique user identifier (UUID) in the LSO for comparison. With a second UUID being tracked, given a reasonably robust analytics package able to count the number of unique values passed into the system, the analyst is able to compare the number of unique visitors based on a browser cookie to the number of UUIDs stored in the Flash LSO.



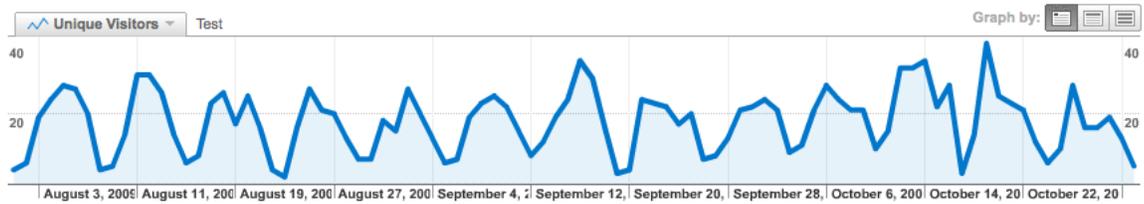
2,233 visits used 676 user defined values in the "Test" segment

Figure 3: Example of Google Analytics used to track 676 unique user identifiers (UUIDs) using the custom variable.

Given that all web analytics packages (Omniture, Unica, WebTrends, Coremetrics, etc.) are actually reporting the count of uniquely counted browser cookies when they report something they call “Unique Visitors,” the two numbers can be used to calculate a “cookie correction ratio” much like the one called for by the Internet Advertising Bureau in the most recently updated Audience Reach Guidelines²⁰.

19 <http://blog.quantcast.com/quantcast/2009/08/flash-cookies-measurement.html>

20 http://www.iab.net/iab_products_and_industry_services/508676/



This custom dimension resulted in 703 Unique Visitors via 92 days in the "Test" segment

Figure 4: Example of Google Analytics tracking for the 676 user defined values tracked in Figure 3 reporting on "Unique Visitors" (which is Google's imprecise term for uniquely tracked cookies)

Using Figure 3 and Figure 4 as an example, the "cookie correction ratio" for this data set would be:

$$703 \text{ cookies} / 676 \text{ unique IDs} = 1.03 \text{ cookies per unique ID}$$

The calculation suggests that, at least for this site, only 3 percent of cookies are being deleted, although it does not tell us how many visitors are doing the deletion. Armed with this simple calculation, an audience measurement specialist can then make the case for accepting cookie-based audience counts or use the value to "correct" reported counts, whichever the business prefers. While this approach does not resolve the cookie deletion issue with the same elegance of the reset strategy, it does provide additional information required to improve the accuracy of audience measurement without putting site operators in the position of being accused of disrespecting consumer privacy. Given the reality of cookie deletion, Web Analytics Demystified believes this is the most responsible approach even though not necessarily the most beneficial to the business.

If you must use Flash Objects to reset browser cookie values, Web Analytics Demystified strongly recommends disclosing the practice. Weather.com is doing an admirable job of this on their web site, although they are unfortunately vague about the technology involved (Figure 5).

guidelines/audiencemeasurement

We have developed a simple mechanism that allows us to protect some of your custom settings -- even if your weather.com cookies are deleted -- by saving a backup of certain cookie values to a different location on your computer. We can then simply reset these saved values to your cookies when you revisit the site, allowing you to continue enjoying your customized experience on the weather.com website and on other products and services from The Weather Channel. You may [enable or disable this functionality](#) at any time. If you disable this functionality and your cookies are deleted, you won't have access to many of the features which make your experience more efficient and some of our services will not function properly.

Figure 5: Excerpt from Weather.com privacy policy outlining the use of Flash Local Shared Objects to reset browser cookie values in the case of their deletion (from <http://www.weather.com/common/home/privacy.html>)

Additionally, if you do provide for this functionality, we strongly recommend giving visitors a simple strategy to opt out. Weather.com also offers a good example of how this opt-out can be managed if Flash-based cookie reset is enabled (Figure 6).

Would you like for us to remember you if your cookies are deleted?

We have designed this functionality to improve your experience on weather.com and in other products and services from The Weather Channel. If you select **"Yes"** below, we will be able to reset some of your custom settings if your cookies are deleted.

If you select **"No"** below, we won't be able to reset your custom settings if your cookies are deleted. If you disable this functionality and your cookies are deleted, you won't have access to many of the features which make your experience more efficient and some of our services will not function properly. You can always update your preference via our [privacy policy](#).

Would you like for us to remember you if your cookies are deleted?

Yes No

Figure 6: Page on the Weather.com web site that allows the consumer to disable tracking and reset enabled by Flash Local Shared Objects (from <http://www.weather.com/common/help/flcookieforgetme.html>)

Again, because there is a general tendency to want to hide the use of Flash to reset browser cookies, and because it is unlikely the general public will respond positively despite educational efforts to communicate the value of the strategy, we believe that Flash Objects should not be used to reset browser cookies.

Given the strategy described above for generating a key calculation, in Web Analytics Demystified's opinion, the risk is not worth the reward in this situation.

Disclose the Use of Local Shared Objects

In addition to using Flash Local Shared Objects appropriately, Web Analytics Demystified strongly recommends disclosing their use as clearly as possible. The obvious location to communicate this is in your site's online privacy policy, and we recommend either working with a certification organization like TRUSTe or at least using language similar to theirs. Following is text you can use which is based on TRUSTe's policy, modified slightly by Web Analytics Demystified:

DISCLOSURE OF THE USE OF FLASH OBJECTS FOR TRACKING

This site uses Flash Local Shared Objects (LSO), also known as "Flash cookies," to store some of your preferences, to display content based upon what you view, to personalize your visit, or to otherwise track your activities across multiple visits to the site. Third Parties, with whom we partner to provide certain features on our site, to display advertising based upon your Web browsing activity, or to track visitor activity and behavior, may also use Flash Local Shared Objects to collect and store information.

Flash Local Shared Objects are different from browser cookies because of the amount of, type of, and how data is stored. Cookie management tools provided by your browser or anti-spyware applications will not remove Flash Local Shared Objects, nor will the "Private Browsing" modes prevent their placement on your computer.

To learn how to manage privacy and storage settings for Flash Local Shared Objects or disable their use entirely please click visit:

http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html

For more information about Flash Local Shared Objects we recommend the Wikipedia entry on the subject:

http://en.wikipedia.org/wiki/Local_Shared_Object

Readers are welcome and encouraged to use this addition to their privacy policy and to modify it to suit their specific needs. And while most consumers *do not* take the time to read privacy policies, Web Analytics Demystified still

believes that disclosure is the best strategy to avoid being vilified in the court of public opinion, especially if your site deals with particularly sensitive or personal information.

Allow Site Visitors to Disable Local Shared Objects

In addition to disclosing the use of Flash Objects, Web Analytics Demystified strongly recommends giving visitors the ability to disable their use programmatically without making them attempt to navigate the Flash Player Settings Manager shown in Figure 2. While the Settings Manager is certainly appropriate for power users and those consumers wishing to disable Flash Objects in their entirety, our feeling is that it is more appropriate to give consumers the ability to opt out of tracking on a site-by-site basis with the simplest tools possible.

To this point, in addition to the Weather.com examples shown in Figure 6, we would refer readers to the opt-out provided by the video tracking service Visible Measures (Figure 7). Visible Measures depends heavily on the use of Flash Objects because their service is based fully on Flash-based video players and has no access to traditional browser cookies. They are using a fully anonymous user ID, tracked in the Local Shared Object, while showing respect for consumer preference by allowing a “one-click” opt-out to tracking across the entire network of Visible Measures tracking.

Viewer Settings Manager

The control below shows your current Visible Measures Viewer Settings and provides relevant options for opting-out or, if you have already opted-out, opting back in if you so choose.

You have a Visible Measures ID

Click here to:

All changes will go into effect immediately. If you have changed your Visible Measures Viewer Settings, please refresh this page and the control will reflect your changes.

For more information about the terms and conditions surrounding the collection and use of information about our users, please refer to our [Privacy Policy](#). If you have questions regarding this policy or the Visible Measures Viewer Settings Manager, please email us at privacy@visiblemeasures.com

Please note: This control currently does not affect any browser cookies set by the visiblemeasures.com sub-domain, which are used exclusively for measuring traditional visits to the Visible Measures Web site. Future versions of the Visible Measures Viewer Settings control may provide additional options for opting-out of these cookies as well.

Figure 7: Flash Object settings manager from Visible Measures, offering a simple explanation and a “one-click” opt-out of all Flash-based tracking across all customer domains (from <http://corp.visiblemeasures.com/viewer-settings/>).

Visible Measures also encourages their clients to disclose the use of Flash Objects and provides language they recommend adding to existing privacy policies similar to that shown in Figure 8.

2. What is Visible Measures' practice regarding cookies?

Like many common online video services, our technology uses Flash-based "cookie" technology (technically referred to as **local shared objects**) to customize and enhance your online experience. These are pieces of information transferred to your computer's hard drive when you visit a site that automatically identify your browser(s) to the server whenever you interact with video content on the site. Visible Measures may combine information obtained through the use of local shared objects with other aggregate or anonymous data, including a unique ID number assigned to you.

You may choose to opt-out of Visible Measures' local shared objects via the Visible Measures **Viewer Settings Manager**. If you do so, that opt-out will be effective for all Visible Measures-enabled sites.

Figure 8: Visible Measures privacy policy discussing the use of Flash Local Shared Objects ("Flash-based cookies", from <http://corp.visiblemeasures.com/privacy-policy/>)

Conclusions

Audience measurement is a critical aspect of any business's online efforts and is fundamental to the evolution of consumer interaction in the digital world. Without accurate numbers and reliable systems, business owners are left with little more than guesswork and "gut feel" to guide them in an increasingly competitive and fragmented environment. The accuracy of many audience measures depends on browser cookies, an often maligned but ultimately harmless text file that is unfortunately blocked and deleted by enough of a segment of the population to reduce the efficacy of the technology.

In response to the decline in accuracy of audience measurement systems resulting from cookie deletion, an increasing number of site owners are turning to a less fragile system, Flash Local Shared Objects (LSO). These objects are essentially "super-cookies" which are dramatically more resilient than cookies due to their implementation and a general lack of knowledge about their existence among consumers.

In Web Analytics Demystified's opinion, the use of Flash Local Shared Objects is unfortunately a risky business. There is strong evidence that more and more companies are using LSOs in direct conflict with consumer preferences and existing systems designed to control access to information and protect a user's privacy online. With the attention given to consumer privacy on the Internet at both individual and governmental levels, we believe that companies making inappropriate or irresponsible use of the Flash technology are very likely asking for trouble (and potentially putting the rest of the online industry at risk of additional government regulation.)

Our recommendations are to be thoughtful and careful about how Flash objects are used in audience measurement. If they are to be used at all, business owners need to ensure that:

- A) they are not used to over-ride consumer preferences;
- B) consumers are made aware of their use via normal channels (e.g., privacy policy);
- C) consumers are given an easy way to opt-out of their use as a tracking mechanism.

While these recommendations may be somewhat controversial within the audience measurement community, we firmly believe that the line between using Flash to improve accuracy and using Flash in conflict with consumer preferences is black and white. Until Adobe, the creators of Flash, more clearly addresses the use of Flash as a tracking mechanism, the onus is on measurement specialists and business owners to do what is right.

The author welcomes feedback on this document. Please feel free to write Eric T. Peterson (Web Analytics Demystified) at eric.peterson@webanalyticsdemystified.com.

About the Author

Eric T. Peterson

Eric T. Peterson, CEO and Principal Consultant at Web Analytics Demystified, has worked in web analytics since the late 1990's in a variety of roles including practitioner, consultant, and analyst for several market-leading companies. He is the author of three best-selling books on the subject, *Web Analytics Demystified*, *Website Measurement Hacks*, and *The Big Book of Key Performance Indicators*, as well as one of the most popular web analytics bloggers at www.webanalyticsdemystified.com.

Mr. Peterson has committed much of his life to the betterment of the web analytics community, so much so that Jim Sterne, President and co-founder of the Web Analytics Association says "Eric's leadership in the industry is unparalleled, his devotion to the community is legendary and his years of experience translate immediately into strategic and tactical competitive advantage for everybody who works with him."