Market View

A New Cookie Cutter for Classifying Web Cookies

Summary
Recent industry reports and newspaper articles have documented users' increasing deletion of third-party Web cookies, and the resulting inaccuracy when measuring Web visitor behavior. However, the pundits' use of technology-oriented terms such as "first-party" and "third-party" cookies is obscuring the end user point-of-view that is driving this change in behavior. The cookie controversy needs a new vocabulary — "single site," multi-site," "enabling," "monitoring" — to clarify the issues.

What Is a Cookie?
Netscape introduced cookies as a way to help Web sites preserve user state during a Web visit. Unlike a business application such as Order Processing, which remembers who the user is and whether the user has finished a transaction (e.g., entering an order), a Web server is "stateless." That is, it sends out a Web page whenever one is requested, and doesn't know that the Web page that it just sent out is related to the Web page it sent out two minutes ago. To preserve this concept of "state" as (IT folks would call it) or "session" as laypeople would call it, Netscape invented cookies in the mid-90s. A Web server initially sends these small text files to a user's Web browser, and then trades them back and forth with the browser for the remainder of the session. The Web browser deletes a temporary, or "session" cookie, when the session with the Web site ends; the browser saves "persistent" cookies to the PC's hard drive for retrieval during a later session by the Web server that created them.

Engineers and pundits often characterize cookies based on which type of Web site sets them: e.g., "first-party" or "third-party." A first-party cookie is set by the site that the user is visiting — for example, the Web site of Classmates.com. A third-party cookie is set by a third-party site providing a service to the main Web site. In the Classmates.com case, this would be a cookie from Omniture, a Web analytics company, and cookies from three ad networks (Bluestreak, Claria, and ValueClick).

A first-party cookie sometimes contains personalization information — for example, a user name and a logon ID, so that a user is automatically recognized when he or she visits a site. If cookies didn't store such information, sites would have to re-ask a user's name or preferences whenever the user came back to the site, for example.

However, third-party cookies often offer less direct value to the user. The Omniture cookie tracks a visitor's path through the site, so that Classmates.com can optimize the site over time by monitoring which pages are popular and which pages prompt people to leave the site. The ad network cookies track user behavior across multiple sites, helping ad networks characterize a user's behavior. This makes it easier for them to display ads to a target segment of users: for example, frequent visitors of sports sites. However, this multi-site aggregation of information about a visitor, even if the visitor remains anonymous, is what has privacy advocates in an uproar.

The End User's Action: Deleting Third-Party Cookies
Largely because they can, browser vendors now discriminate between first-party cookies and third-party cookies in their Options menu. Rather than rejecting cookies altogether, for example, a user can accept first-party cookies and reject third-party cookies. In fact, rejecting some third-party cookies (those without a compact security policy or those that use personally identifiable information without implicit consent) is Internet Explorer 6.0's default policy. (In Internet Explorer 5.5, Microsoft introduced the "Delete all cookies" button on the primary Options page.) These evolving browser capabilities, along with the growth of programs such as McAfee's Anti-Spyware program, have been behind users' increasing blocking of third-party cookies. This increased deletion of third-party cookies (Jupiter Research pegs the number at around 39% a month) has created havoc in the Web analytics space. Users deleting cookies en masse makes it appear to a Web site that the number of new visitors is increasing and the number of return visitors is decreasing. In short, that the site is experiencing different visitor behavior, when in fact it isn't.

The Enterprise Reaction: First-Party Cookies and Local Shared Objects
To counteract that resulting skew, on-demand Web analytics companies have been moving to enable their cookies to be set by their client's Web site (first-party), rather than their own third-party site. While not preventing all inaccuracies — for example, users can still delete all of their cookies or move to a different PC — it does attack the highest priority problem. In addition, there's a backup solution. Jupiter Research is suggesting companies investigate using Macromedia Flash Local Shared Objects (LSOs) as a cookie replacement/backup. Like a Web cookie, a LSO is a text file, and only the Web site domain that created it can read it. However, from an enterprise's point-of-view, a LSO offers an extra benefit — since it isn't a cookie, standard browsers don't delete it, anti-spam programs don't delete it, and users rarely know how to delete it manually. Therefore, at least at the moment, it is much more persistent than a cookie. The typical, non-techie user is outfoxed again.

However, given past behavior, this will be a short term victory. For example, The Electronic Privacy Information Center (www.epic.org) is already warning about Local Shared Objects, and there is now an add-on available for Mozilla Firefox (named Objection) that lets users delete LSOs from the Firefox Options panel.

Needed: A New Vocabulary
The market is at this juncture because it has simplistically lumped cookies into two classifications: first-party and third-party cookies. This technological classification system obscures the reasons end-users are keeping or deleting cookies: users see some cookies as adding value to the browsing experience, while others are viewed as a privacy invasion. Put simply, the industry needs to move to a new vocabulary that reflects the conceptual framework that users are using to decide whether to keep or delete cookies. Implicit in this naming convention is the assumption that a user will avoid deleting a cookie that offers clear, specific benefits to the user, and eagerly delete one that passes intelligence on to a Web site with no corresponding benefit for the user. Because this is a more complex problem than hinted at by the "first-party" and "third-party" terms, it requires a more complex vocabulary.

A cookie has three characteristics:
1. *Universe* — Whether it tracks behavior for a single-site (single-site) or a network of multiple sites (multi-site), such as for an ad network. Note that only third-party cookies can track behavior across multiple sites.

2. *Goal* — The main process goal of the cookie. For example, is it set to save work for the user, by remembering a password and preferences (enabling), or is set to enable the Web site to track visitor behavior (monitoring)? A single site can set both types of cookies.
3. *Source* — Which type of Web site set the cookie? The site the user is visiting (first-party) or an affiliated site (third-party)?

Table 1: A New Web Cookie Vocabulary

End-User Perceived Value	Collection Universe	Process Goal	Server Source	Example	Description
High	Single-site (cookie tracks behavior for a single site)	Enabling (saves work for the user)	First-party	Amazon.com	Amazon stores visitor information and preferences to allow Web site personalization and recommendations .
			Third-party	Clickability, used on Nascar.com	Nascar.com uses Clickability to generate Save This, Print This, and other buttons on its site (Clickability also monitors use of those buttons for Nascar.com).
Minimal	Single site	Monitoring (watches behavior; no immediate end-user benefit)	First-party	American Express.com	American Express uses Web analytics software (e.g., Sane) to monitor user behavior.
			Third-party	Omniture, used on Classmates.com	Classmates.com uses a third-party Web analytics service (e.g., Omniture's SiteCatalyst) to monitor user behavior.
Threatening	Multi-site (cookie tracks behavior across multiple sites)	Monitoring	Third-party	Bluestreak, Claria, and ValueClick, used by Classmates.com	These ad networks collect Web browsing behavior as a way to offer relevant ads.

Source: Ballardvale Research

With This New Vocabulary, User Behavior Is Now Clearer
With this more sophisticated cookie vocabulary, the gradations of user worries about cookies become clearer. The most worrisome are third-party cookies, largely because some of them — not all — have the ability to track user behavior across multiple sites. Because browsers and anti-spyware programs have classified all third-party cookies as hostile, users delete them — including the less worrisome third-party cookies that track user behavior for a single site. (While on-demand Web analytics vendors perform visitor tracking for multiple clients, they keep the data from different clients separate — site A can't see the traffic data for site B, and vice versa. This is analogous to ADP, which in the brick-and-mortar world performs payroll processing for many companies, but keeps the payroll records separate.)

Furthermore, such deletion-happy end users suffer no ill effects, because all third-party cookies are cookies that monitor — that is, they offer no immediate value to the end-user. It's the individual Web sites, trying to watch user behavior as a way to ultimately improve site navigation and better target their marketing, that suffer.

This suffering is what's causing Web analytics vendors to migrate from third-party to first-party cookies. However, even that shift is not a safe haven, and will not be until companies use cookies as a way to optimize the user's Web site experience, or even require it for doing business. A user who deletes Amazon's cookies, for example, suddenly loses a lot of the power of the site — personalized recommendations and one-click ordering. As a more severe example, McAfee — which makes a business out of deleting Web cookies — points out that it cannot offer certain services (e.g., WebImmune) to people who delete its own cookies.

Ballardvale Conclusions
End users should continue what they're doing — deleting cookies if they feel they are worrisome. This is a personal decision — some people worry about leaving even a trace of what they've done on the Web, others could care less, and most people are apathetic.

While enterprises should migrate to first-party cookies to survive the current crisis, they should take a longer term view and think through the value of personalizing their site for the end-user. Such personalization will not only increase visitor loyalty, it's also a way for companies to decrease cookie deletion and thereby maintain more accurate visitor measurement. After all, it's only when the cookie offers value to the end-user that he or she will think twice about deleting it. And, at least at the moment, cookie names are frequently so arcane that a user will leave all of the cookies from the site to preserve enabling capabilities, rather than ferret out which one is for personalization and which one is for monitoring.

In the end, the Web is similar to the brick-and-mortar world — users are willing to offer up information about themselves as long as they get something worthwhile in return. Without that equitable balance — if Web visitors live in a world of "take, take, take" cookies that pull information but offer no compensating ease-of-use in return — Web users will view the "cookie relationship" as one-sided, inequitable, and one that should be terminated.

© 2005, Ballardvale Research. All rights reserved. Reproduction without the express written consent of Ballardvale Research is strictly prohibited. Information is based on best available resources. Opinions reflect the analyst's judgment at the time and are subject to change. This report was downloaded from www.ballardvale.com.