

ELECTRONIC PRIVACY INFORMATION CENTER

Local Shared Objects -- "Flash Cookies"

Introduction

[Cookies](#) are small text files used to save information about an individual or their use of a web site. For instance, a cookie can be used to save your login name, your preferences for viewing content, or to track you as you browse the Internet.

With the advent of spyware and spyware removal programs, as well as media attention and the increase of online literacy, users now understand the purposes and risks of using cookies. Recently, users have become more vigilant in purging cookies from their computers. According to a [Jupiter Research study](#), 58% of online users have deleted cookies from their computer and 39% of users do so on a monthly basis. This regular "cookie tossing" is causing direct marketers to see more invasive methods to track individuals. One of those methods is to set a "Local Shared Object," also known as a "Flash cookie" to track individuals. Simply put, the idea behind this tracking is to set two cookies on the user's machine--a standard cookie that the consumer may erase, and a second Flash cookie that the user probably will keep, because the existence of Flash cookies is not well known.

Flash cookies are set through a mechanism in Macromedia's Flash MX player. According to Macromedia, 98% of computer have some version of Flash on their computers.

What is a Local Shared Object (Flash cookie)?

Using previous versions of Flash, developers could save information between sessions by using 'normal' cookies, but the process was considered difficult for developers to implement. Placing a normal web cookie requires the use of a scripting language outside of Flash (Javascript or ASP, for example). Placing a Local Shared Object only requires the use of ActionScript--the scripting language that controls Flash movies. In its newest version, Flash MX, Macromedia introduced the Local Shared Object, which provided an easier way to store information. Flash cookies can be considered to be equivalent to 'normal' cookies, save for a few minor differences.

Flash cookies provide the only method by which a flash movie can store information on a user's computer. Intended uses of the object include storing a user's name, a favorite color or the progress in a game. The actual information is stored in a .SOL file in a special directory on the user's computer. Using the [flash configuration tool](#), the user can decline Flash cookies by domain as well as control the amount of data a site is allowed to store. By default, sites are permitted to store 100kB of information without prompting a user.❖

Unfortunately, few consumers are aware of where Flash cookies are stored or how to control their use. Normal web cookies can be managed via the preferences dialog of most web browsers, but no similar utility is included for these Flash cookies. It is possible for Flash cookies to remain on user's computer indefinitely, as there is no mechanism to set an expiration date on Flash cookies.

How do Flash cookies allow Identification on individuals?

The type of information stored in a Flash cookie is limited only by the information that the creating Flash movie has access to. According to Macromedia's [Flash MX Security Whitepaper](#), this is limited to:

- Anything in the actual movie file

- Any information the user provides
- Some configuration information about the computer running the movie
- Flash cookies created by the same domain from which the movie originated
- Servers in the domain from which the movie originated

Using some or all of the above categories, the Flash movie can create a unique ID and store that ID in a Flash cookie on a user's computer. The Flash movie can then communicate this information to a database, or other applications. Subsequent visits by the same users could be tracked by reading the ID contained in the Flash cookie.

Who can access a Flash cookie?

As with normal web cookies, a domain can only access data that it created; it is not allowed to read Flash cookies created by other domains. This prevents sites from observing user behavior at other sites.

How can users prevent Flash cookie tracking?

Like normal cookies, Flash cookies are represented as small files on users' computers. To prevent Flash cookies from being placed, users can adjust preferences on a per site basis in the [Macromedia Website Privacy Settings Panel](#). Using this tool, Flash cookies can be completely disabled or allowed on a per domain basis.

To get to the settings panel, right click on any Flash movie, click settings and then advanced. Macromedia has published a [walk through guide](#) to help users disable Flash cookies.

Users can get rid of the current Flash cookies and their tracking information simply going to the correct folder (see below) and deleting them. The Flash cookies are organized in folders according to the site that placed them, so users can choose which objects to keep.

Firefox users can use [Objection](#), a recently developed extension that adds a LSO deletion tool to Firefox preferences.

Where are Flash cookies stored?

Flash cookies are stored in a special directory depending on the operating system on the client machine. They are arranged in directories according to the site that placed them on the computer (look for a file with a .SOL extension):

- Windows C:\Documents and Settings\[username]\Application Data\Macromedia\Flash Player
- Macintosh OSX /Users/[username]/Library/Preferences/Macromedia/Flash Player
- GNU-Linux ~/.macromedia

Persistent Identification Element ("PIE")

[United Virtualities](#) (UV), an online marketing firm, has introduced a tracking platform that takes advantage of the relative obscurity of Flash cookies. In a [press release](#) this March, UV announced PIE, a backup ID system for cookies. Mookie Tenenbaum, founder of United Virtualities, explained the reasoning behind the product, "All advertisers, websites and networks use cookies for targeted advertising, but cookies are under attack. According to current research they are being erased by 40% of users creating serious problems."

UV's press release also claims that the PIE system can restore deleted web cookies. Although there is little official information on the implementation of the PIE system, it is not likely that the cookie is actually restored. Instead, it appears that the Flash cookie acts as a redundancy. That is, the PIE system uses Flash cookies as a backup. A site interested in tracking a user would set a normal cookie

and a Flash cookie. If the user erased the normal cookie, the PIE-enabled site could use the redundant Flash cookie to track the user.

To justify this tracking mechanism, UV's Tenenbaum said, "The user is not proficient enough in technology to know if the cookie is good or bad, or how it works."

This practice is highly deceptive. By deleting cookies, consumers are clearly rejecting attempts to track them. Using an obscure technology to subvert these wishes is a practice that should be stopped. Cookies have many beneficial purposes and can make the end user's web experience better. Websites should be honest and up front about how they use cookies, and they should respect the decisions of those users who do not want to be tracked via cookies.

News

- Tessa Wegert, [The Web cookie is crumbling and marketers feel the fallout](#), The Globe and Mail, July 21, 2005.
- Matt Marshall, [Escalation in the Cookie Wars](#), The Mercury News, April 18, 2005.
- Michael Cohn, [Flash Player Worries Privacy Advocates](#), InternetWeek, April 15, 2005.
- [Tool can resurrect deleted cookies](#), Out-Law.com, April 5, 2005.
- Roger Park, [United Virtualities Develops ID Backup](#), iMedia Connection, April 1, 2005.
- Antone Gonsalves, [Company Bypasses Cookie-Deleting Consumers](#), InformationWeek, March 31, 2005.

Resources

- Macromedia.com, [How to disable Local Shared Objects](#).
- Trevor Zion Bauknight, [Cookies and PIE An Introduction to Flash Security](#), Cafeid.com.
- Waleed Anbar, [Your Privacy and Macromedia Flash Player](#), Macromedia.com.

[EPIC Privacy Page](#) | [EPIC Home Page](#)

Last Updated: July 21, 2005

Page URL: <http://www.epic.org/privacy/cookies/flash.html>