December 1997

Innovations Affecting Us-The Cookie Monster: Personal Privacy and the Internet

Judy Luther

Norman Desmarais
Providence College

Sandra K. Paul
SKP Associates

Albert Simmonds
R.R. Bowker

Follow this and additional works at: <https://docs.lib.purdue.edu/atg>

Part of the [Library and Information Science Commons](#)

Recommended Citation

Luther, Judy; Desmarais, Norman; Paul, Sandra K.; and Simmonds, Albert (1997) "Innovations Affecting Us-The Cookie Monster: Personal Privacy and the Internet," *Against the Grain*: Vol. 9: Iss. 6, Article 34.
DOI: <https://doi.org/10.7771/2380-176X.2897>

This document has been made available through Purdue e-Pubs, a service of the Purdue University Libraries. Please contact epubs@purdue.edu for additional information.

Innovations Affecting Us — The Cookie Monster: Personal Privacy and the Internet

by **Norman Desmarais** (Providence College) <normd@sequent1.providence.edu>

Column Editors: **Norman Desmarais** (Providence College <normd@sequent1.providence.edu>

Judy Luther <jluther@earthlink.net>

The tragic death of **Diana, Princess of Wales**, brought to international attention the value that some people put on personal privacy and the measures they will take to preserve it. Few, if any, of us will ever have to worry about paparazzi besieging us or invading our privacy. But that doesn't mean we can become complacent in our anonymity.

We all know that most of the messages we send over the Internet have about the same level of security as the common postcard. Even though efforts are underway to develop greater security measures and encryption techniques for communications on the Net particularly for business transactions, they are still far from finding widespread use. In addition, there are unobtrusive ways for business people, marketers, and others to get information about us without our realizing it. Our Web browsers even facilitate this.

The Cookie Jar

Just about all Web browsers incorporate features that support "cookies" which permit tracking our Net surfing habits. A cookie consists of encoded data that a server sends to a client, such as a Web browser. This information is stored on the hard drive of the end user's computer for later retrieval. Cookies are not programs and cannot be executed nor do they carry viruses. In certain circumstances (determined by the data in the cookie itself), the cookie could return the information it gathers to the server that originally delivered it without first receiving a specific request.

Behind the scenes, Web servers keep logs of the type of system and browser we use as well as where we've come from. In some cases, they can obtain even more detailed information. To see what kind of information a cookie can track, point your browser to the **Center for Democracy and Technology's** site <www.cdt.org> and click on the Privacy Demonstration.

An active Web transaction using HTTP protocol is "stateless." This means that each connection is "fresh" and the server has no knowledge of any other HTTP transaction because it does not store any information about a particular transaction.

A cookie, on the other hand, maintains "state" information which consists of data about a communication between a user and a server. That data could consist of an identification number that tracks a user from one visit to another, the current time and date, or some other piece of information. Cookies can generate profiles of a user's visiting habits — monitoring what pages one visits and what one likes to access. Thus, they allow Web sites to maintain information on a particular user across HTTP connections.

Cookies have many similarities to option settings in desktop software or to personal profiles, such as frequent flyer profiles, kept on corporate computers. For example, a frequent flyer profile might store a client's name, address, and phone numbers;

preference for aisle or window seats; preferred method of payment; and credit card numbers. Cookies store information in much the same way.

A Web server sends information to the client's hard drive when returning an HTTP request made by the client. The file can contain a description of the range of URLs the client accessed within the site. It can also contain fee and registration information, user IDs, a listing of purchases, as well as credit card numbers. Cookies can be designed to expire after a certain time or after a user's visit is over. They can also be set up so that they are sent only via a secured channel.

Cookies are passive data structures that can't be larger than 4K. They are delivered to the client, stored on the client's hard drive, and can be read only by the Web site that sent them. Once a Web site has sent a cookie to a system, it can track the recipient's movements through the site. When one returns to the site later, it knows that the client has been there before. To see how cookies work, link to <<http://www.geocities.com/Athens/Acropolis/1017/cookie.htm>>. After you reload the page, you will see how the cookie keeps track of your visits and gives you a new message with each visit.

Cookie Uses

Cookies have been used primarily for storing online ordering information, tracking site navigation, and personalizing Web pages. A Web site may use cookies to track what advertisements the client has seen and make sure that he or she sees only ads not seen before. Or it may show more ads similar to those previously viewed. Cookies cannot be used to gather sensitive information such as the fields in a Web browser's preference file or in other files stored on the computer. They can be used, however, to store any information that the user volunteers, such as by filling out an HTML form, for example.

When shopping online, it is preferable to store purchases in a "shopping cart" to buy all the items together instead of one at a time. Filling out a Web form with name, address, and other information can facilitate subsequent connections so one does not have to repeat it every time one connects to a site. The information is stored and automatically uploaded so one doesn't have to provide it repeatedly. We frequently use signatures on our email messages without giving it a second thought. Yet, these signatures contain information similar to cookies.

Cookies can serve to store information about articles, such as their URLs and their corresponding charges; so the searcher can pay for them all at once rather than each time he or she downloads an article. Web sites that require a user name and password can issue a "guest pass" in the form of a cookie when the server successfully verifies a user name and password. This could allow access to certain areas of the Web site for a specified amount of

continued on page 88

International Dateline

from page 83

lic Library for Science and Technology of Russia and the Scientific Library of Moscow State University were developing their own in-house systems, but none of these libraries were working on cooperative projects with each other and had definite opinions (usually poor) about each other's systems. One thing that appears to be universal is ego. It is very difficult to find common ground among all the development being done by individual institutions. However, most libraries were consistent about their opinions regarding a vendor from outside Russia — too expensive and not enough experience.

Moscow seemed to be a little more affluent than St. Petersburg; the roads were better; unfortunately the traffic was worse. I aged a great deal in Moscow just by driving through the city. Our first day, we went to Red Square and it was there I immediately fell in love with the city. St. Basil's Cathedral was to one side with Lenin's tomb on the other and Kremlin Square in the background. I fell in love with the onion-shaped domed cathedrals which were ubiquitous throughout the city. New cathedrals have been built since the fall of the communist government, but they don't have the soul of the cathedrals built in the fourteenth and fifteenth centuries. Most of these cathedrals were undergoing restoration since they were used for storage and left in disrepair during the communist period. Our guide, Tonia, pointed out a beautiful little church in downtown Moscow that she remembers visiting as a child when it was an exotic fish museum.

We had the chance to talk to professors at the **Moscow State University of Culture** which is where librarians are trained. Students enter the University right after secondary school and

the library program takes five years. I don't know if it was comforting or depressing to learn that the library profession worldwide seems to be a low-paying profession. Librarians in Russia don't make much money and many of the graduating students are working in commercial arenas because the money is much better.

I think one of the most humbling things I noticed there was the graciousness with which we were received. We were a motley crew of librarians — none of us were particularly well-known in the library community or from prestigious institutions, yet they took us through some of the oldest and largest libraries in Russia. At each library we were met by the Deputy Director or the assistant director. We met the heads of departments responsible for collections of millions and millions of items and every person we met was very kind and was genuinely happy to have us there.

Upon arrival in Russia, I felt like I'd landed on a different planet. Part of this could be blamed on that dopey feeling that comes from jet-lag, but everything appeared so different — the language, the street signs, the food, and even the libraries. By the end of the trip, many things still appeared different — my Russian pronunciation was still dreadful, and I never did acquire a liking for borsch, but I felt like I was back on planet Earth and the way people enjoy their work I suppose many things are pretty much the same wherever you go.

NB: This article will also appear in the *Ameritech Library Services Newsletter*. — KS

Innovations

from page 87

time. After the set time period, the guest pass expires and the visitor must log in again.

Web designers are interested in how visitors navigate around their sites, which pages they visit most frequently, how they enter those pages, and whether navigation can be made more efficient. Cookies can track this kind of information on a user-by-user basis, in addition to providing information for shopping carts and site personalization.

Sites like *The New York Times* <www.nytimes.com> use cookies to replace site login which forces users to enter a user name and a password every time they log on to the site. That data is stored in a cookie instead.

Filling the Cookie Jar

There are only two ways to store client data. Either the server provides it or the user provides it by taking some action, such as clicking a link or button or filling out a form. Marketers and site managers gather demographic information in this way to build user profiles. Magazine publishers, among many other businesses, create cookie files based on such user profiles. Proponents of using cookies in this manner argue that it isn't much different from what many supermarkets do with discount cards or what sales and marketing departments do with responses to telephone solicitations or direct mail campaigns.

The same information stored in a cookie can be stored just as easily on a server by using a simple server-side application that stores user information in a database. However, many people

consider this practice of gathering personal information for use in corporate databases or for cookies an invasion of their privacy. After all, every time a searcher downloads a Web page, the browser sends the Web server information about what Web browser and operating system the client uses, the URL of the last page visited, and the computer's IP address. That's a lot of personal information; and every browser sends it every time one clicks on a link.

The controversy about cookies comes from the fact that they place information on the hard disk and that they function in the background, mostly without our knowledge. We're all wary of somebody tampering with our hard drives; and how many of us even know we have a "cookie jar" there? Cookie information can travel to databases via CGI scripts, enabling server owners to use that information any way they choose. As cookies pass information back and forth with each visit, they eventually build detailed user profiles, which are often used by third parties to deliver targeted advertisements to Web site visitors. Many people fear that if servers can send a cookie to a visitor's computer, what else can they send? A virus, bug, or other type of application?

Putting a Lid on the Cookie Jar

Web browser producers are working on improving their browsers to alert users when their computer is receiving a cookie. **Netscape's Network Preferences** option (under the Protocols tab) lets users select whether or not to show an alert before accepting a cookie. Tighter security features are also under development; but what can individuals do to protect themselves in the meantime?

Although it's difficult to avoid cookies altogether, it's not

continued on page 89

impossible. First of all, network surfers can remove cookie files by deleting Netscape's Cookies.txt file or **Internet Explorer's** Cookies directory. However, this will require re-registering at a Web site the next time they wish to access it. It may also result in the loss of any customized features.

If they send electronic forms that contain sensitive information, such as a credit card number or a mailing address, they can transmit the cookie data in the context of a Secure Sockets Layer session which encrypts the information as it travels between the client and the server (e.g. as set in Netscape's Network Security options).

There are also programs, called cookie managers, that have emerged to help users deal with unwanted transmissions. One type of manager blocks all cookies, refusing them without asking. A second type intercepts the transmission of any cookies and alerts users, allowing them to accept or reject the cookie. A third, more sophisticated type offers more options, such as blocking cookies from specific sites or deleting cookies individually.

Barefoot Productions's Cookie Master <www.hotfiles.com> or <http://www6.zdnet.com/cgi-bin/texis/swlib/hotfiles/info.html?code=000CKP> provides access to each cookie in addition to cookie files and directories. It is convenient and easy to use and doesn't work in the background.

Scott McDaniel's Crumbler 97 <www.scsescorp.com/personal/scottmac> revisits Cookies.txt every 45 seconds and automatically deletes any cookies it finds. It does not delete cookies selectively, so it can quickly become overkill, destroying cookies that one may want to keep.

Cookie Crusher is one cookie manager that analyzes incoming cookies immediately and accepts or rejects them in real-time based on one's preferences. It is especially useful because a user can make a list of sites that should and should not be allowed to set cookies. This feature gives freedom to trusted sites yet still protects one's browsing privacy. **Cookie Crusher** can be configured to reject all cookies automatically as well. The program can keep a detailed list of the cookies accepted and rejected from all servers for the current session. An added option permits saving the list to a file for later perusal. A free 30-day trial version is available from **The Limits Software** <ftp.thelimitsoft.com> or <ftp.blackcat.net> (both in Massachusetts), from <www.oz.net> (Washington), from <www.euclidmachine.com> (California),

or from <volftp.tin.it> (Italy).

Kevin McAleavey of **NSClean Privacy Software** <http://www.nsclean.com>, a division of **Privacy Software Corporation (PSC)** of Albany, NY has designed **IEClean32** (for **Microsoft Internet Explorer**) and **NSClean32** (for **Netscape Navigator**). These programs get rid of cookies in the browser and can erase all record of news group activities, including the list of those visited or subscribed to. The programs can also delete the history database, clean out cache files, and even obliterate the URL list in the windows showing the pages one has visited. The programs cannot monitor these functions in the background, however. It will require some manual activity to effect this cleanup. Although future versions of the programs will include a feature to let users choose which specific records in a group (such as bookmarks) to delete, **IEClean32** and **NSClean32** currently cannot do this. Nor do they permit hiding records rather than destroying them. Nevertheless, they are comprehensive solutions for covering one's online tracks.

Pretty Good Privacy Inc.'s PGPCookie.cutter for Windows NT <www.pgp.com> offers complete control over which cookies clients allow, which ones they refuse outright, and which ones they collect so they can decide about them later. This is a wise approach to security. A Windows version may become available soon. UNIX users can use the **Internet Junkbuster Proxy** <http://www.junkbusters.com/ht/en/ijb.html> to control cookie access. **Cookie Jar** <http://www.lne.com/ericm/cookie_jar/>, on the other hand, lets them select the URLs they want to block from sending cookies. This program must be run under a UNIX machine and must use a browser that supports an HTTP proxy.

Other programs that readers can explore to protect themselves from unwanted cookies include **Kookaburra Software's Cookie Pal** <www.kburra.com> which uses a tabbed dialog box to show all cookies stored and **Luckman's Anonymous Cookie for Internet Privacy** <http://www.luckman.com/anoncookie/anoncookiebody.html>.

Some programs do a better job of cleaning up after themselves than others, creating opportunities for programs like **SoftDD's Complete Cleanup** <members.aol.com/softdd>. **Complete Cleanup** gets rid of the debris other programs leave behind, such as cache files, history files, and cookies; but it does not let users choose which items to delete and which to keep.

Another alternative to collecting cookies is to use the **Anonymizer Web site**

<http://www.anonymizer.com>. This service prevents cookie files from being created while browsing. A similar service, **Lucent Personalized Web Assistant** or **LPWA** <www.lpwa.com>, acts as a middleman between a Web browser and Web servers. It is designed specifically to work with sites that offer personalized information without sacrificing the user's privacy. Once a client logs on to the LPWA server, the searcher can visit sites anonymously. Only the LPWA can trace the client's true identity.

A lot of personal user information travels over the Internet in each transaction with no security protection. As the theft of user identities becomes an increasingly serious problem, Net surfers have reason to be wary of the cookies they collect and what might occur with their personal information after visiting some sites. Researchers who do online research on controversial issues such as abortion, birth control, capital punishment, or gun control might find themselves subjected to harassment from special-interest groups. Their user information may get sold or traded to other interested parties that might bombard them with junk mail based upon their Web activities, whether or not these activities are representative of their search habits.

Somebody might also stumble accidentally upon a porn site, as happened to me when a combination of quick clicks took me away from a job applicant's online resume instead of to a desired link. A

cookie manager can prevent the installation of a cookie that would permit tracking one's browsing activities. Surfers have a variety of products to choose from and more will undoubtedly be developed. For more information on privacy issues on the Internet and the role of cookies, see **Viktor Mayer-Schoenberger's** article, "The Internet and Privacy Legislation: Cookies for a Treat" in the *West Virginia Journal of Law and Technology* <http://www.wvjolt.wvu.edu/issue1/articles/mayer/mayer.htm> and the **Electronic Privacy Information Center's Cookie Page** <http://www.epic.org/privacy/internet/cookies/>. **Malcolm's Guide to Persistent Cookies** <http://www.worldwidemart.com/scripts/cookie/lib.shtml> is an excellent guide to cookie resources.