

What Everybody on the Internet Knows about You

by Boris Loza, PhD, CISSP

Application(s): Netscape Navigator 4.7 and above

Operating System(s): Solaris

You'd probably be surprised if you knew what information about yourself is available on the Internet! Do you want to know what kind of information? Go to <http://www.leader.ru/secure/who.html> or <http://www.anonymizer.com/snoop.cgi> and check it out. If you can't wait, look at **Figure A** for a sample.

Figure A: This is a snapshot of the information provided by one of the many "Internet security" sites.



As you see, they can find out where you've come from (your IP address and domain name), your operating system (Solaris 2.6), browser type (Netscape v4.76), and many other things. Besides this, many servers keep careful records of your input into search engines, information that's submitted in forms, your shopping habits on the Web, and information about uploaded/downloaded files.

Who gets this information and how?

Some companies, such as Doubleclick, create large databases of such information, which are used by target advertising companies or can be sold to any interested buyers. Have you ever wondered why every copy of Netscape running on Microsoft Windows defaults to

<http://www.netscape.com/> as a home page and Internet Explorer browser defaults to <http://www.msn.com/>?

Another method that Web sites use to track visitors is a special file called a cookie, which contains a small amount of information transmitted between a Web server and a browser. Cookies can contain your username/ID, computer type, IP address and server location.

Ever heard of Web bugs (also known as clear GIFs)? Like cookies, Web bugs are electronic tags that help Web sites and advertisers track visitors' whereabouts in cyberspace. The placement of a Web bug on a page allows the site hosting the banner ad to know your IP address and the page that you visited. This can be further correlated to cookie information that may be sent by your browser as part of the request to retrieve the page. But Web bugs are invisible on the page and are much smaller, about the size of the period at the end of this sentence. Unlike cookies, people can't see Web bugs and anti-cookie filters won't catch them.

Browsers also contain other useful data for those who know how to make use of it, such as hit logging and GUID numbers, as used by Microsoft's Internet Explorer. Hit logging keeps track of all of your offline activities. When you click on a banner ad, a record is made of how long you looked at it and what ad you clicked on, as well as personal information stored by the IE browser. Hit logging is also designed to "phone home" to the server that created it.

GUID numbers are randomly generated "Guaranteed Unique" or "Globally Unique" ID numbers. It's highly unlikely that these numbers will ever occur twice across the planet. They are the ultimate "electronic dog tag" and can survive even if you kill the cookies and remove the "spyware."

Since the GUID number is kept on your system, it can be requested at any time. And since Microsoft has it on its databases—along with your name, address and other registration details—the potential for creating a system that tracks your every online move is enormous. And there's even more! Did you know that if you're on a network, every Office 97 file you create can be traced back to you? That's because Office 97 kindly attaches its own permanent GUID to everything you create. So if you send a document to Sally and she deletes its entire contents, replaces it with abuse about the boss, adds a macro virus to it, renames it and sends it to everyone in the company, it's still got your address on it as the originator. You can see what GUID looks like by opening any Office 97 Word file with Notepad and searching for the phrase GUID. A few bytes later, you'll find an ID number broken up with spaces inside two curly braces. By the way, GUID helped to capture a creator of the Melissa virus. But that's another story.

Other applications and companies that use "spyware" and "phone home" are RealNetwork's RealJukebox, PKZip, zBubbles, CuteFTP and many others. SurfMonkey is an application that's supposed to block Internet sites inappropriate for kids, but it also keeps their personal ID, phone

number and email address. Radiate is a company that serves the shareware market. Popular applications such as GO!Zilla, Free Solitaire and GetRight come embedded with an automated ad-serving "spyware" package created by Radiate. More than 400 different applications have this program embedded within them.

The Comet Cursor from Comet Systems is cursor software that replaces the standard screen cursor with many funny-looking cartoon characters that appeal to kids, such as Garfield and Pokemon. This is free software, but while users think they're getting just a cute cursor, in reality every time they visit any of 60,000 Web sites supporting Comet Cursor technology, it will report the user's unique serial number back to Comet Systems. Therefore, a profile of the user's interests can be compiled, and targeted ads can be served up to the users. (There's no such thing as a free lunch!)

In this article, we'll show what you can do to minimize, and sometimes prevent, submitting information to the Internet on your behalf. Even if you continue to allow it to happen, at least you'll be aware of how they do it.

Cookies and Web bugs

When you revisit an Internet server, your browser shares the cookie previously installed on your hard drive, providing information that quickly identifies you. Whenever you hit a Web site supported by advertising, the ad server reads the cookie from your machine. The ad server then uses your cookie to look up your profile and determine which ad to serve to you dynamically, based on the interests it's gleaned from your surfing activities at its member sites. The ad server also records which advertisements you've clicked through. The type of ad and the amount of time you've spent at the site is also captured. Also keep in mind that cookies, the subject of several lawsuits, are sent in clear text, in both directions, whenever encryption isn't used.

You can see your cookies by opening the `.netscape/cookies` file in your home directory. The Netscape cookies file is also shown in [Listing A](#).

Listing A: *Netscape's cookies file*

```
# Netscape HTTP Cookie File
# http://www.netscape.com/newsref/std/cookie_spec.html
# This is a generated file! Do not edit.

.sun.com      TRUE / FALSE 996868914 sun_visitor_uid      363431
3033313431305e30
```

```

.passport.com      TRUE / FALSE 2145744038 MSPDom      2

.hotmail.msn.com  TRUE / FALSE 2145744412 HMP1  1
.msn.ca           FALSE / FALSE 1065294038 MC1      V=2&GUID=7ebfd
6b436de4f0f9f0e17cac673c5a0
.rambler.ru       TRUE / FALSE 1308339742 ruid     DFP2BeOqLzsJVAAAA
WSaBUT1v

.amazon.com       TRUE / FALSE 993628838  session-id 103-
5876521-
2065404

.amazon.com       TRUE / FALSE 2082787243 x-
main             hQFiIxHUFj8mCscT@Yb5Z7xsVsOFQjBf

.netscape.com     TRUE / FALSE 1293839990 UIDC      295.127.207.85:
0993043901:206454

.altavista.com    TRUE / FALSE 1388491200 AV_USERKEY AVS03872b
75251d100a2020160095754

.doubleclick.net  TRUE / FALSE 1924991999 id       80000007

```

This file consists of a block of ASCII text. Briefly, what you can see in this file is (based on the first row):

- **Domain.** The domain that created and can read the variable (.sun.com).
- **Flag.** A TRUE or FALSE value indicating if all machines within a given domain can access the variable (TRUE). This value is set automatically by the browser, depending on the value set for domain.
- **Path.** The path within the domain for which the variable is valid (/).
- **Secure.** A TRUE or FALSE value indicating if a secure connection (like SSL) with the domain is needed to access the variable (FALSE).
- **Expiration.** The UNIX time at which the variable will expire. UNIX time is defined as the number of seconds since Jan 1, 1970 00:00:00 GMT (996868914).
- **Name.** The name of the variable (sun_visitor_uid).
- **Value.** The value of the variable (3634313033313431305e30).

Note that most cookies can be accessed by all hosts in the domain (e.g., .sun.com, .hotmail.com, etc.). For more information about cookies, browse Netscape's Cookie Spec located at http://www.netscape.com/newsref/std/cookie_spec.html.

The easiest way to protect yourself from cookies is to disable this feature by choosing Edit | Preferences | Advanced from the Netscape menu. But some Web sites (such as

<http://www.hotmail.com/>) require cookies. You can fool such Web sites by deleting the cookies file and replacing it with a link to /dev/null:

```
ln -s /dev/null cookies
```

In this scenario, all cookies are accepted, but no information is stored on your hard drive.

The Web bugs, like cookies, are usually used for tracking customer habits, but are much harder to detect. A Web bug is a graphic on a Web page or in an email message, that's designed to monitor who's reading the page or message. Unfortunately, this technique could be used toward malicious ends, such as grabbing IP addresses or installing files. The security company Security Space, in a monthly report

(http://www.Securityspace.com/s_survey/data/man.200105/webbug.html), has identified companies that benefit from the use of Web bugs, including online advertising networks DoubleClick and Linkexchange, as well as Yahoo and America Online.

The only way to find a Web bug using the Netscape browser is to view the HTML source code of a Web page and search for IMG tags that match up with cookies stored on the user's computer. A Web bug typically has its HEIGHT and WIDTH parameters in the IMG tag set to 1; it's loaded from a different server than the rest of the Web page; and it has an associated cookie. For example:

```
 =>border=0 width=1 height=1>
```

This Web bug was placed on the home page by Rumbler.ru to provide "spy" information about visitors to Spylog.com.

Email Web bugs are also represented as 1-by-1 pixel IMG tags just like Web bugs for Web pages. However, because the sender of the message already knows your email address, they also could include the email address in the Web bug URL. The email address can be in plain text or encrypted.

Web bugs used with emails allow the measurement of how many people have viewed the same email message in a marketing campaign. They help to detect whether someone has viewed a message. (People who don't view a message are removed from the list for future mailings.) They also help to synchronize a Web browser cookie to a particular email address, allowing a Web site to know the identity of people who come to the site at a later date.

For a demonstration of a bugged Yahoo profile, see <http://profiles.yahoo.com/webbug2000>. This profile contains a visible Web bug image that's being loaded from a server other than Yahoo. The

Web bug provides a log of everyone who has visited the profile page. For more information, check The Web Bug FAQ at http://www.eff.org/pub/Privacy/Profiling_cookies_webbugs/web_bug.html.

Unfortunately, at this time, no application software is available to detect Web bugs for Netscape running on UNIX. As a result, you need to be careful of the sites you visit.

Proxies, anonymity providing servers and remailers

One can remain anonymous while Web surfing by using a proxy server. A proxy acts as an intermediary, routing communications between clients and the rest of a network. Web proxies can hide your IP address and allow you to stay anonymous. If you don't use any proxy server yet, you may choose one from a Free Proxy Public Servers List at <http://tools.rosinstrument.com/proxy> or <http://proxys4all.cgi.net/>. To configure your Netscape browser to use a proxy, go to Edit | Preferences | Advanced | Proxies. Under Manual Proxy Configuration | View, put the host name of the proxy you're going to use and a port number (provided by proxy server). To check whether your proxy server reveals your IP address, go to <http://www.all-nettools.com/pr.htm>. If you get the message Proxy server is detected!, then there's a security hole in your proxy, and information about your real IP address is listed. (In this case, try to use another proxy.) If the message is Proxy server is not detected, everything should be OK.

If you don't want to use a proxy server, try one of the Anonymity Providing Servers listed in **Table A**. These servers act as a proxy, since Web pages are retrieved by them rather than by the person actually browsing the Web (you). Go to one of these Web sites and just type a URL you want to visit—the server does the job for you, securing you from many potential dangers.

Table A: *Some of the Anonymity Providing Servers available*

Available servers	Web address
Servers with SSL support	
SafeWeb	http://www.safeweb.com/
Rewebber	http://www.rewebber.de/ and http://www.anon.de/
Servers without SSL support	
Anonymouse	http://anonymouse.is4u.de/
Aixs NET	http://www.aixs.net/
Anonymizer	http://www.anonymizer.com/
SiegeSoft	http://www.siegesoft.com/

SafeWeb uses 128-bit SSL encryption for all HTTP data, which prevents your ISP from tracking your Internet activities. The only traces that are left from your browsing are in your browser history list.

If you want to remain anonymous while sending emails, you can use a remailer. This is a special service that receives an email message from you, then readdresses it and sends it to the person you want to send it to. During the process, any headers that might point back to you are removed. Many remailers are available on the Internet; some of them let you put a fake return address, but most of them directly state that the message is sent from an anonymous source. One of these Web-based remailers can be found at <https://ssl.dizum.com/help/remailer.html>. For a list of remailers check <http://security.tao.ca/email.shtml>.

Other useful tips

Banner ads can be a nuisance, and can also give third parties another method to track your Web use. To get rid of these ads, update your `/etc/hosts` file by putting in the following lines:

```
127.0.0.1 ad.preferences.com
127.0.0.1 ad.doubleclick.com
127.0.0.1 ads.web.aol.com
127.0.0.1 ad.doubleclick.net
etc.
```

This causes your Web browser to look up an offending domain in a black hole (your loopback address). All you'll see after this is a blank rectangle where the ad used to go. You can block any other Web sites from your users this way (pornography, violence, etc.). A pretty big list of such Web sites can be found at <http://dc.gamershq.com/hosts.txt>. Just be careful to check all Web sites on the list prior to blocking them.

You may also want to clear out your browser's History list. This is something that should be done each time you're finished with your browsing, if you don't want someone to be able to easily see where you've been surfing (if you share your Solaris workstation or server). If you use Netscape, simply delete the `~/netscape/history.*` files at the end of your session.

Another place that your Web trail is recorded is the cache directory—a temporary storage area for recently visited pages and images (`~/netscape/cache`). The cache allows for repeatedly visited Web sites to show up more quickly when you reload them into your browser. If you don't want people to read your cache files, they should be deleted. Note, however, that on slower machines with slow connections, this will result in a noticeable decrease in the speed when your computer

brings up previously visited Web pages. To delete your cache, select Edit | Preferences | Advanced | Cache from Netscape's menu bar and click the Clear Disk Cache button. There you can set your Disk Cache to OK if you prefer (which means that pages you view are never cached).

Balance your paranoia

This article isn't intended to frighten you. Just remember that there isn't much privacy on the Internet. So think carefully about which sites you choose to visit, and think twice before you provide any information about yourself.