

By Carole Levitt and Mark Rosch

Protecting Your Privacy on the Internet

Use of the Internet means exchanging data between your computer and other computers

Many Internet users—even relatively sophisticated ones—tend to think that surfing the Web is like surfing the channels on the television, but there is a significant difference. When people watch television, their particular viewing habits are not recorded without their knowledge. When they surf the Internet, their surfing habits can be and probably are. Often without fully realizing it, Internet users are exchanging a range of information with the sites they visit and leaving an easy-to-follow trail of informational crumbs.

Information that identifies individual Internet users, their surfing habits, and even their passwords can be gleaned from a variety of sources, including the records of Web sites they have visited that are stored on their own computers and the information they leave behind at the Web sites they visit. This information may be recorded by those Web sites they visit, by third parties that are accessing their machines from remote locations, or simply by sitting down at their computers when they are not present.

In order to access the Internet, every computer is assigned a unique Internet Protocol (IP) address. When accessing the Internet from home (or from a firm that does not have a network), the IP address is assigned by an Internet Service Provider (ISP), such as AOL or Earthlink. In a networked corporate setting, each computer's IP address is assigned by the IT manager. Every request by the user's browser to a Web site being visited leaves a record of the IP address on that site's Web server. While IP addresses from commercial ISPs are not assigned permanently to the user (as they typically are on a corporate network) and do not show your e-mail address or your name, an ISP can match (by reviewing login records) a specific IP address that it assigned at a specific time to a specific user.

This lack of privacy understandably concerns many computer users. As a result, a number of services exist to cloak a user's Internet activity. By using a service such as Anonymizer (www.anonymizer.com), users can anonymously access any Web site and leave behind the IP address of the server of the Anonymizer company rather than their own. To use Anonymizer's

free cloaking service, users type the Web address of the site they wish to visit into the address box on the Anonymizer.com home page. The only downside to this free service is enduring the advertisement for the pay ver-

sion of Anonymizer displayed at the top of each site visited. A one-year subscription without the advertisement and with additional security features is available for \$29.95. The Cloak (at <http://www.the-cloak.com>) and Go Proxy (www.goproxy.com) offer similar services to users who are concerned with their privacy.

Hidden Spyware

In 1999, the FBI loaded "key logger" software onto the computer of reputed organized crime figure Nicodemo Scarfo Jr., recording every keystroke made on his computer. This allowed the FBI to capture some of Scarfo's passwords, which in turn allowed them to decipher information from the encryption software he was using. In that case, the judge ruled that such key logging did not constitute an illegal wiretap. (Visit <http://lawlibrary.rutgers.edu/fed/html/cr00-404-1.html> for more information.). Similar software, which "hides" on a hard drive once it is installed, can be purchased for \$50 to \$200. Originally designed to monitor the Internet activity of children and allow government and corporations to track the computer use of employees, key-logging software is increasingly being used by spouses. Computer users should know, therefore, that a parent, spouse, or employer with access to their computers (and that may include remote access) can install software that tracks and reports their every keystroke. Spector Soft (one manufacturer of spy software) has placed a warning in its software's license agreement that "requires that you inform anyone you may

monitor with Spector Soft products." Users who fear for their privacy may not conclude that this clause entirely relieves their worries, however.

Spector Soft is not the only vendor of computer spyware. Desktop Surveillance (www.datarecoverysoftware.com) and Investigator (winwhatwhere.com) also record browser activity and track every program opened, every file saved, and every keystroke (including passwords). One application, Eblaster (found at <http://www.spectorsoft.com/purchase/eblaster.htm>), even sends a screen shot, via e-mail, whenever the user being tracked uses the computer on which it is installed.

Electronic Footprints

Even without hidden spyware, an ordinary computer offers a wealth of data to those who know where to look. Microsoft's Internet Explorer and Netscape's Communicator keep a record of Web sites that the user has recently visited. The History file, which is stored on the computer's hard drive, conveniently allows users to look back at a list of recently visited sites without having to bookmark or remember a site's Web address. The History file is not password protected; therefore, someone who leaves a computer turned on but unattended makes this information available to anyone else who accesses the computer.

The History file can also yield important forensic evidence. For example, Washington, D.C., police reviewed the History file on Chandra Levy's computer when searching for clues that her

Carole Levitt and Mark Rosch are principals of Internet For Lawyers. They can be reached at levitt@netforlawyers.com.

Statement of Ownership, Management and Circulation

UNITED STATES POSTAL SERVICE
(Required by 39 USC 3685)

1. Publication Title: Los Angeles Lawyer
2. Publication Number: 01622900
3. Filing Date: October 1, 2002
4. Issue Frequency: Monthly (Except combined July/August)
5. Number of Issues Published Annually: 11
6. Annual Subscription Price: \$14.00 member; \$28.00 nonmember
7. Complete Mailing Address of Known Office of Publication: Los Angeles Lawyer, 261 S. Figueroa Street, Suite 300, Los Angeles, CA 90012-2503
8. Complete Mailing Address of Headquarters or General Business Office of Publisher: Los Angeles Lawyer, 261 S. Figueroa Street, Suite 300, Los Angeles, CA 90012-2503
9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor. Publisher: Samuel L. Lipsman, Los Angeles Lawyer, 261 S. Figueroa Street, Suite 300, Los Angeles, CA 90012-2503. Editor: Samuel L. Lipsman, Los Angeles Lawyer, 261 S. Figueroa Street, Suite 300, Los Angeles, CA 90012-2503. Managing Editor: Samuel L. Lipsman, Los Angeles Lawyer, 261 S. Figueroa Street, Suite 300, Los Angeles, CA 90012-2503. Contact Person: Samuel L. Lipsman. Telephone: (213) 896-6503
10. Owner: Los Angeles County Bar Association, 261 S. Figueroa Street, Suite 300, Los Angeles, CA 90012-2503
11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities. None
12. Tax Status. The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes: Has Not Changed During Preceding 12 Months.
13. Publication Name: Los Angeles Lawyer.
14. Issue Date for Circulation Data Below: Sept. 2002
15. Extent and nature of circulation: (Column 1: Average No. Copies Each Issue During Preceding 12 Months. Column 2: No. of Single Issue Published Nearest to Filing Date.)

	Column 1	Column 2
a. Total Number of Copies (Net Press Run)	22,116	21,350
b. Paid and/or Requested Circulation		
(1) Paid/Requested Outside-County Mail Subscriptions Stated on Form 3541	20,743	20,460
(2) Paid In-County Subscriptions Stated on Form 3541	0	0
(3) Sales Through Dealers, Carriers, Street Vendors, Counter Sales, and Other Non-USPS Paid Distribution	0	0
(4) Other Classes Mailed Through the USPS	138	135
c. Total Paid and/or Requested Circulation	20,881	20,595
d. Free Distribution by Mail	202	190
e. Free Distribution Outside the Mail	0	0
f. Total Free Distribution	202	190
g. Total Distribution	21,083	20,785
h. Copies Not Distributed	1,033	565
i. Total	22,116	21,350
j. Percent Paid and/or Requested Circulation	99%	99%
16. This Statement of Ownership will be printed in the November 2002 issue of this publication.
17. Signature and Title of Editor, Publisher, Business Manager, or Owner: Samuel L. Lipsman, Publisher and Editor. Date: 10/1/02. I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including multiple damages and civil penalties).

Web use may have inadvertently left behind. They discovered the Web request for a map to the park in which her remains were eventually found. Internet Explorer's History can be viewed by clicking the History tab on the Navigational tool bar. Netscape Communicator's History can be viewed by clicking on Communicator on the Menu Bar, scrolling down to Tools and then selecting History.

Many Web sites also employ cookies as a means to identify visitors. A cookie is a small piece of information that the site being visited places on the visiting user's local hard drive. Ostensibly, cookies are intended to function as a means to expedite a user's return visits to favorite sites or personalize the information received from a site. For example, many users are familiar with how Amazon.com uses a cookie to identify returning visitors by name and to recommend products for purchase based on their prior buying history with Amazon.

Most cookies include the address of the site that placed them on the user's computer. These addresses, in turn, may be accessed by other Web sites to track the user's general Web usage, identifying sites the user has visited and perhaps even the user's passwords for those sites. Cookies can also be accessed and deciphered by someone who sits at your computer and knows where to find the cookie file. Newer versions of Communicator and Explorer can be configured to warn users before cookies are added to their computers. This gives users the option of deciding whether or not to allow cookies to be placed on their computers. Users who enable this option may be surprised how many sites employ cookies, and how some sites employ multiple cookies.

Cookies are not only placed on users' computers by Web sites that users visit but also by third-party advertisers featured on those Web sites. One can opt out of receiving third-party cookies from two of the largest online advertising clearinghouses by visiting Network Advertising Initiative (NAI, which is found at http://networkadvertising.org/optout_nonppii.asp).

Data Collection

This summer, the largest of these advertising clearinghouses, Double Click, settled a two-year investigation with the attorneys general of 10 states regarding the way Double Click collected and used identifying information about Web users. (See the agreement at www.oag.state.ny.us/press/2002/aug/aug26a_02_attach.pdf.) As part of the settlement, Double Click promised not to combine information it gathers (from cookies generated by various ads) to create de facto

master profiles for individual Web users. Double Click is also developing a means by which Web users will be able to view the information about themselves that Double Click has compiled.

The most reliable and effective way of gathering personal data, however, remains simply to ask for it. Many Web sites offer free content or prizes in return for registration. Just as the amount of information requested of a user varies from site to site, so too do the intentions of the sites gathering this information. Before entering personal information into a Web site, be sure to read the site's privacy policy. If the site does not have a link to its privacy policy prominently displayed near a form requesting information, one should be wary of supplying any information.

There are a number of other practices you can employ to protect your privacy:

- To discover if someone has placed key-logging software on your computer, programs such as Hook Protect ([visit downloads-zdnet.com.com/3000-2092-10025791.html](http://www.downloads-zdnet.com.com/3000-2092-10025791.html)), Spy Guard (www.spyguard.com), and Spy Cop (www.spycop.com) claim to be able to detect and eliminate hidden key loggers.
 - Periodically, clear your history files so no one can view your surfing history.
 - Use the Cookie Manager in your browser to clean out unnecessary cookies already on your computer and to warn you when cookies are being placed on your hard drive.
 - Also, set the Cookie Manager to reject third-party cookies.
 - Install a firewall to protect against hackers.
 - Shut down your computer when you are not using it so no one can view your history or cookies.
 - Install a password to open your computer, so no one will be able to access your computer after it has been shut down.
 - Use the free Anonymizer. If you download the pay software, your name is registered and you may be tracked if a court order is issued.
 - Before entering any sensitive data (e.g., a Social Security or credit card number) into an interactive Web form, be sure you are in a secure and trustworthy site: Check that the address begins with "https" rather than "http" and a small locked padlock icon appears in the lower left corner of the browser's window.
- As a final precaution, computer users may simply keep in mind that computers are designed to store, copy, and share information with great speed and efficiency. These capabilities may always be exploited in ways that will dismay a particular user. Users may take significant steps to protect their privacy online, but the best advice may be: If you want to keep it a secret, don't do it on the Web. ■