Dynamic Chiropractic

NEWS / PROFESSION

Protecting Yourself on the Net, Part 2

WHO DO YOU TRUST? PRIVACY ON THE WORLD WIDE WEB

Michael Devitt

Of the 100 sites tested, about half automatically collected personal or computer data about the people who were visiting the sites.

"A cookie is a small chunk of information that can be planted into your computer when you visit a website, and used without your knowledge."

A person's right to privacy on the Internet has become a hot topic of debate. Earlier this year, several of the Net's leading data collection agencies agreed to voluntary limits to minimize the invasion of privacy. They agreed that from now on, they would release personal information (such as a user's social security number, buying preferences, household income, and other data) only to "qualified subscribers" who promise to use the information appropriately. Previously, such information was available to any party that was interested in acquiring knowledge about an individual.

While this may sound like a great relief to many, the actions of these companies represent the exception rather than the rule. The fact is that there are hundreds of such organizations out on the Internet, all selling personal information to whoever is interested. With the right resources and some financial reserves, just about any type of information on anyone can be acquired. The scary thing is, much of this information is being gathered, bought and sold without our knowledge or consent.

An EPIC Test of Privacy

In June, the Electronic Privacy Information Center (EPIC) surveyed the 100 busiest Internet sites to see how they operated in terms of user privacy and the ability to gather information. The sites were ranked by the 100hot.com web service. Some of the sites mentioned (Amazon.com, ESPNet, etc.) are ones that many of you probably frequent.

The results were startling. Of the 100 sites tested, about half automatically collected personal or computer data about the people who were visiting the sites. Only about a third of the sites mentioned that they were actually doing such a thing.

Concerning privacy and protecting the information you disclose, only 17 sites even mentioned the privacy factor. Most of those came up short of what EPIC terms adequate disclosure: for instance, explaining why information is collected, how that information will be used, and what steps the site will take to limit improper use of the data. And only eight sites gave users some control over whether the website could share information with other companies or individuals.[1]

Marc Rotenberg, director of EPIC, sees a problem with the way that information is obtained and can be used. "If a person goes to the website and gives up his or her name, that person is not necessarily going to know how that information will be used, or if there will be any safeguards to protect that person's privacy, and we think that's a problem."[2]

The Internet's "Cookie" Monster

Whenever you enter a website, your computer sends the site some kind of information: usually the type of computer and operating system you're using. However, your computer can also be asked about what other parts of the Net it's visited lately, and what it was doing there.

Many websites enable the creation of "cookies." Basically speaking, a cookie is a small chunk of information that can be planted into your computer when you visit a website, and used without your knowledge. Almost a quarter (23) of the sites surveyed by EPIC used cookies. None of the sites bothered to mention that little fact to their users.[3]

When a user first visits a website and gives out personal information, the site's computer creates a cookie and stores it in the user's hard drive. This way, when the user next visits the site, the cookie will be retrieved, and the site will greet the user by name (and/or their e-mail address).

The problem with this is that the same technology that creates cookies can also be used to track other information as well. A cookie can track which sites a person visits, what pages a user looks at, etc., and then link the data to that person's name and address. Site owners can then sell the information to advertisers and other third parties, all without the user's knowledge or consent.

Some Internet browsers can be configured to notify the user when a cookie is set and let you choose whether or not to accept a cookie. Although this option offers some privacy, the process of surfing the Web slows down to a crawl. Instead of automatically accepting cookies, a user has to manually accept or reject them, and this option doesn't stop once you enter a site.

Some sites have cookies attached to each page you visit. For example, ESPNet contains as many as 2,500 separate pages on its website, most of which have their own cookie. Imagine the time it would take to browse the complete site while choosing to accept or reject cookies on each page. In addition, because the default settings on Netscape Navigator and Internet Explorer are automatically set to accept cookies, many users are not aware of this feature. And as stated before, most sites that use cookies do not even mention it to users.

The Big Test: What Does the Net Know About Me?

Even after starting this article and reading other pieces that had been published about Internet privacy, I didn't think the powers that be knew all that much about me. Sure, like most people, I'd submitted my name and address to a few websites without thinking. I'd spent time in chat rooms and newsgroups posting messages, talking with people from all over the world. And I'd purchased a few hard to find CDs and books off of the Internet last fall.

But I'd always followed the guidelines friends and other users told me. I didn't give out information to shady-looking websites. I asked my name to be taken off e-mail lists. I enabled my web browser to alert me to incoming cookies from other websites. And I made sure that any financial transactions done over the Net were done with a secure protocol. I was safe, right?

Wrong! Here's some of the information that was available about me:

- full name, date of birth, gender, and marital status;
- personal address and telephone number;
- personal e-mail and world wide web addresses;
- mother's maiden name (I'd used it as a password once);
- name of my high school football team (I'd used that as a password, as well);
- high school I graduated from, and year of graduation;
- university I'm currently enrolled at, and my major;

- how many e-mail messages I've sent and received in the past week;
- time spent connected to the Internet for the past month;
- names of the CDs and books I purchased off of the Internet in November of 1996;
- titles of two movies I rented from Blockbuster Video three months ago.

That's what I was able to find out for free. For a small fee to a data collection service, I could have found out a lot more, such as:

- my social security number (yes, they are for sale);
- personal driving record and any records of criminal activity;
- credit history, estimated yearly income, and other financial information;
- medical history, including the name of my doctor and any medications I may be taking;
- type of residence I live in;
- how long at my current address;
- type and amount of campaign contributions made to any political parties;
- addresses and phone numbers of my relatives;
- identities, addresses, and telephone numbers of my 10 closest neighbors.

This experience was a bit unnerving. Finding out the information took just a couple of phone calls and an hour or so of actual work. All it took to find out this much data was a name, telephone number, and e-mail address. What if someone had a grudge against me and wanted to find out everything they could? With access to the Internet and some extra money, who knows what else they might find.

Protecting Yourself

So how do you make sure important information like your credit history, medical records and social security number don't fall into unscrupulous hands? Here are a few options:

1. Enable your web browser so that it alerts you about accepting cookies from web sites. On Netscape Navigator, this is done by accessing the network preferences section from the options menu; in Internet Explorer, you can access the cookies folder. The newest version of Netscape Navigator allows users to turn off the use of cookies altogether.

2. If you receive a lot of junk e-mail, send a message back and ask to be taken off that group's e-mail list. Many companies are notoriously slow when it comes to doing this, so you may have to send several messages for them to get the point. If that doesn't do the trick, complain to your Internet service provider. After enough users complained to America Online about junk e-mail, they announced a ban on e-mails sent from five Internet message service companies.

3. Don't post your e-mail address on newsgroups. Use your first name only, then wait and see who replies. Better yet, post you messages through an anonymous remailer. This service hides the heading of an e-mail message, allowing you to post messages while making the name and address of the sender indecipherable.

4. Buy and install privacy/encryption software. A number of companies sell encryption software that keeps websites and other organizations from finding out personal information about you.

A decent privacy program for people who use Netscape Navigator is Internet Fast Forward, available for a free trial at [url=http://www.privnet.com]http://www.privnet.com[/url]. Among other privacy features, this plug-in allows users to block websites from sending cookies and advertisements banners. Users might also want to try an encryption program called Pretty Good

Privacy. The commercial version sells for about $129, but you can download a freeware version at [url=http://www.pgp.com]http://www.pgp.com[/url].

There are dozens of other encryption programs available, and the list is growing rapidly as privacy becomes a larger factor. Some programs come as part of a suite of software programs (e.g., the Stronghold program on Helix Software's Nuts and Bolts); others, like McAfee's PCCrypto and NetCrypto, offer powerful features for encrypting and decrypting sensitive information before it gets sent as an e-mail attachment or file.

Online Help

In addition to the programs and hints suggestions above, there are a number of websites worth visiting that deal with the privacy issue:

Electronic Frontier Foundation ([url=http://www.eff.org]http://www.eff.org[/url]): The site is dedicated to the protection of privacy, free expression, and public information on the Internet. The site contains updates on the online free speech and privacy campaigns, and links to other privacy organizations.

Electronic Privacy Information Center ([url=http://www.epic.org]http://www.epic.org[/url]): The site contains the June 1997 survey they conducted on data collection and provides other valuable information about privacy on the Internet.

Stalker's Home Page ([url=http://pages.ripco.com:8080/~glr/stalk.html]http://pages.ripco.com:8080/~glr/stalk.html[/url]): This site, the personal creation of Glen L. Roberts, provides numerous links to information databases and other data collection agencies. It's a great resource because everything's on one page for you.

The information provided in this column is not intended to scare any of our readers away from getting online, but to show the awesome power of the Internet, and how easily private information can be made public without one's knowledge or consent. If you are concerned about your right to privacy online, please contact EPIC or the Electronic Frontier Foundation and voice your opinion.

As always, we welcome your feedback. If you have any questions or comments about the Internet, or if there's a topic or website you'd like to see reviewed, please e-mail me or call me at the number below.

References

1. The intricate world of the web. CNN Interactive ([url=http://www.cnn.com]http://www.cnn.com[/url]), June 10, 1997.
2. Ibid. 3. Web users seek more privacy. CNN Interactive, June 9, 1997.

Michael Devitt
Huntington Beach, California
Tel: (714) 960-6577
Fax: (714) 536-1482
Editorial@DCMedia.com