InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Five Ways To Keep Your Google Searches Private

Word that the government has been seeking search data from Google has struck fear into the hearts of Internet Explorer and Firefox users. Here are five simple steps to keep outsiders from uncovering private information about your Web browsing habits.

By Alexander Wolfe, TechWeb.com
Feb. 1, 2006
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=178600222

The recent news that the U.S. Justice Department has been seeking search data from Google, Yahoo, MSN, and America Online has struck fear into the hearts of Web surfers. Many users are concerned, not because they're done anything wrong, but because they wonder just how much personal information can be gleaned from their on-line searches.

While the government action is aimed at fighting child porn, some computer-security pundits and newspaper columnists are raising concerns that even users who haven't gone anywhere near such toxic material could potentially have their searches traced.

Political debates aside, the question of browser privacy is at its heart a technical issue. Whether you're using Microsoft's Internet Explorer or Mozilla's Firefox , there are at five simple steps you can take to keep Web busybodies from uncovering information on your search queries.

Delete your history.

This one's easy, and obvious. IE and Mozilla maintains histories of all URLs which are typed into their address bars.

Clearing out the history is simple. Just go into "Internet Options," located under the "Tools" menu in Internet Explorer. (Here's a more detailed explanation from Microsoft.) In Firefox, histories can be clearing by going to "Tools" > "Options" > "Privacy."

That's something Robert Petrick apparently didn't do. During his North Carolina murder trial in November, prosecutors showed that his hard drive contained Google searches for the words: "neck," "snap," "break," and "hold." Petrick was convicted of the first-degree murder of his wife. **Clear out your cache.**

All browsers contain a cache, which is used to store Temporary Internet Files. The cache acts as a kind

of pre-loader for the browser; if a previously viewed page is requested again, it can be loaded locally rather than going out across the 'Net to grab it a second time.

Microsoft itself provides simple instructions on how to clear your cache. It's done by clicking the "Delete Files" button under the "Temporary Internet Files" section of the "Internet Options" dialog box.

Firefox cleans the cache via the same "Tools" > "Options" > "Privacy" path used to ditch the history.

However, some users don't feel that's enough. The reason: while clearing out the cache at first glance appears to get rid of a browser's temporary internet files, it doesn't clear out all remnants of the files. That's because, as is the case for other files on your hard disk, the deletion process only kills pointers to the file's data -- it doesn't physically overwrite the file. (The data's still hidden on the disk, a fact data-recovery tools use to "undelete" lost files.)

For privacy obsessives, obliteration requires a full file wipe. That's essentially what's promised in a host of third party tools, which claim to take cache deletion to the next level.

Bust your cookies.

After history and cache, the third leg of the browser privacy triad is cookies. These are small files Web sites place on your PC to log information on your visits. (The Mozilla Foundation provides a consumer-friendly explanation of how and why sites suck in cookies, here.)

Many Web sites won't let you visit them if you have your cookies turned off, but that doesn't mean you can't periodically clean them out. Microsoft provides easy instructions for cookie deletion.

For Firefox, there's an available "view cookie" add-on that lets users look at who's looking at them. Users looking to consolidate their clean-up efforts can turn to a tool from Microsoft. Though it's called "Clear Cache Feature For Internet Explorer," the program will actually delete all temporary Internet files, cookies, and history files. It was originally developed to help out users plagued by corrupted entries causing IE errors, but it can be used by anyone running IE under Windows XP.

Having to separately delete one's history, cache, and cookies will be a thing of the past in the next version of Internet Explorer. As Microsoft's IE blog notes, Internet Explorer 7, which is currently in limited beta, will include a new all-in-one delete feature. This will get rid of temporary Internet files and cookies along with the history, in one fell swoop.

Aware of such developments, e-commerce providers seem to be looking to stay one step ahead of users' privacy efforts. A recent development in this regard is a cookie-on-steroids technology called the persistent identification element, which burrows more permanently into users' PCs.

Use an anonymous surfing tool.

The latest craze in Web privacy is anonymous surfing. Third party tools configure your brower to use proxy servers, which act as an intermediate client between sender and receiver. This makes it pretty much impossible for sites to figure out where the original user that's pinging them is located (they only see the proxy server).

The Electronic Privacy Information Center has compiled perhaps the most comprehensive list of anonymous surfing tools, though the group is quick to point out that it doesn't endorse specific products.

(EPIC is a privacy advocacy group, in Wash., D.C., which boasts 'Net pioneer Vint Cerf on its advisory board.)

The list of software offerings includes the $30 Anonymous Surfing package from Anonymizer and Guardster, a monthly fee-based proxy site. Public Proxy Servers provides what it says is a list of sites around the world which act as anonymous proxies.

The Cloak, which acts an anonymous surfing proxy, warns users that is will not tolerate any illegal activity and notifies them: "You should assume that we will comply with court orders or subpoenas demanding log files entries, as we do not know our users and therefore cannot mount a legal challenge."

Whether such anonymous surfing tools will continue to thrive is anybody's guess. On first glance, the technology harkens back to the anonymous remailers which thrived in the early days of the Internet. The most famous of these, the Finland-based anon.pinet.fi remailer, was shut down in 1996 amid allegations it had been used to transfer child porn.

Rethink your search strategies.

"If you haven't done anything wrong, you don't have anything to worry about," goes an old saying popular among law enforcement types. (Privacy advocates would disagree.)

Nevertheless, users concerned about privacy in all its forms have one decidedly low-tech form of protection available to them. Namely, stay away from any site you wouldn't want anyone else to know you've visited. (Remember, your spouse is far more likely to see your browser history than some faceless government official who's off stalking serious abuse.)

Some may agree with the sentiment expressed by Cox News Service columnist Todd Powell. "Privacy has become a confusing thing for me," he wrote. "There's a public version of me and a private one."

Like most 'Net users, Powell worries about strangers getting ahold of information he'd think twice about sharing with some family members. To keep that from happening, and to avoid downloading viruses and spyware onto your computer, it's only common sense to be careful where you surf.

For concerned parents, Microsoft provides a Content Advisor tool, which limits childrens' access to a specific list of Web sites you define.