They're watching you: Methods to block nosy Web advertisers

October 29 2010, By Mike Swift

Virtually everything you do online is scrutinized by search engines and advertising networks that evaluate you as a potential customer based on what you search for, the sites you visit and the ads you see -- whether you click on those ads or not.

"It's as though every time you pick up a magazine or a book or you browse a storefront, you might be reading the magazine, but it's reading you back, and the ads in the magazine are reading you," said Peter Eckersley, senior staff technologist for the Electronic Frontier Foundation, a civil liberties organization that monitors the online world.

Marketers argue that "behavioral advertising" -- which serves up ads based on a person's browsing history and demographics -- is good because it produces ads that fit a person's interests. But privacy advocates like Eckersley say the "ubiquitous surveillance" violates "a fundamental civil liberty" -- the right to read in private. Another threat, he said, is that someone else could get hold of your data.

So if everything on the Web has eyes, how do you draw the shades?

Many relatively simple tools, including a suite of privacy tools offered by Google, industry groups like the Network Advertising Initiative and privacy groups like the EFF allow anyone to protect the privacy of a search, to see who is tracking your online browsing, and even to block that tracking.

I recently did an experiment where I instructed my browser to send me a message each time a website tried to set a "cookie" -- cookies are small files stored in your browser when you visit many websites, which can record your site preferences and profile information for advertisers. Within five minutes I turned the alert off; the flood of messages was overwhelming.

The Network Advertising Initiative has a site -- www.networkadvertising.org/managing/opt_out.asp -- that shows you which ad networks have cookies on your browser, and lets you opt out of being tracked, although Eckersley said there are better opt-out tools to use. In my case, of roughly 60 ad networks listed on the site, all but 14 had a tracking cookie on my browser. Looking under the hood of my browser, I could see that everyone from home maven Martha Stewart to Facebook's Mark Zuckerberg was essentially peering over my shoulder in my cubicle. But there are ways to maintain your online privacy.

Google's Ads Preferences Manager allows anyone to see the interest profile created from their search and browsing history, and to block Google's tracking if they chose.

A good way to access the site is through Google's Privacy Center, where the Internet search giant lists its privacy tools. Go to www.google.com/intl/en/privacy_tools.html, then click "Ads Preferences Manager." (While in Privacy Center, also check out Google Dashboard, where you can set the privacy settings of any Google service you use.)

Ads Preferences Manager offers a button that disables the cookie Google uses to track people's browsing history. But Jonathan McPhie, a Google product manager in charge of several of the company's privacy tools, said six of every seven people who visit the site have left their Google cookie in place.

"The importance of offering a tool like this is not to see how many people opt out, but to see how many people we can arm with knowledge," McPhie said. "If I know I can opt out, I might feel more comfortable about being tracked."

The site allows users to choose additional interests, from autos to yoga, if they want to see those ads. Google explains behavioral tracking -- Google calls it "interest-based advertising" -- at www.google.com/ads/preferences/html/about.html .

Google, McPhie said, does not classify people by certain sensitive interest groups, including religion, sexual orientation, health status, political preference and adult content.

Google and Electronic Frontier Foundation also offer tools that allow you to encrypt any Google search so no third party can monitor the terms you are searching for.

Electronic Frontier Foundation offers free software called "HTTPS Everywhere" that allows people using Mozilla's Firefox browser to encrypt communications with a number of major websites, including Google search, Wikipedia, Twitter, Facebook, most of Amazon.com, and the websites of The New York Times and Washington Post. Download at www.eff.org/https-everywhere/ . Eckersley said the main purpose is to block eavesdropping by governments, hackers or anyone trying to listen in on your home Wi-Fi. In some cases, Eckersley said, encryption may also interfere with tracking by advertisers.

Google also now offers encrypted search at google.com/" target="_blank">encrypted.google.com/. The encryption means the search terms a person enters can't be read by third parties trying to access the connection between a searcher's computer and Google's servers. Once you go to another website, however, you're fair game for

tracking.

Another way to limit tracking cookies is to use a privacy mode in your browser called "InPrivate" in Microsoft's Internet Explorer; "Incognito" in Google's Chrome browser and "Private Browsing" in Firefox. In those modes, none of the browsers retain a record of websites visited after a session, nor do they permanently store cookies or temporary Internet files.

In Chrome, users can access Incognito mode by clicking on the wrench icon in the toolbar and choosing "New incognito window." In Firefox and IE, click "Tools" and look for the "private browsing" choice.

There are limits to the protection, however. Your computer won't have a record of your browsing history, but your Internet service provider or employer could still track the pages you visit.

It's also possible to change the settings in your browser to block tracking cookies all the time. Many "first-party" cookies, such as the one that allows your bank to recognize it's you each time you log on to check your balances, are desirable. It's "third-party cookies," those digital tags placed by ad networks when you visit other websites, that track your movements.

Eckersley says he blocks third-party cookies, but the downside is that some major websites don't work properly with cookies disabled.

If you want to give it a try, blocking all third-party cookies takes a few more steps. In the Chrome browser, for example, you click the wrench icon on the toolbar, choose "Options," and pick the tab labeled "Under the Hood." Now click the "Content Settings" button, click "cookies" and click the box labeled, "Block all third-party cookies without exception."