https://www.wsj.com/articles/SB10001424052748703467304575383203092034876

WHAT THEY KNOW

How to Avoid the Prying Eyes

The Internet is rife with surveillance technology, but you can cover some of your tracks

By Jennifer Valentino-DeVries

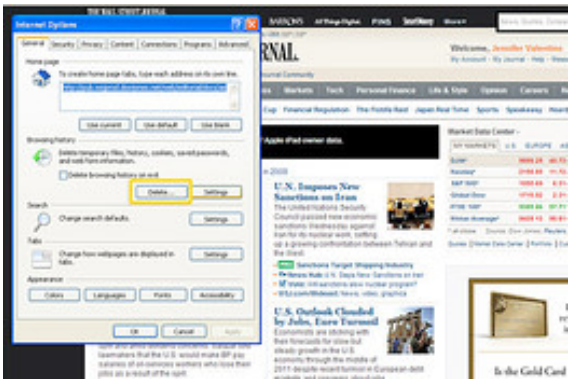
Updated July 30, 2010 12:01 a.m. ET

Visitors to almost every major website are tracked online, a Journal investigation has found. But there are ways to limit the snooping.

STEP BY STEP

Almost every major website you visit is tracking your online activity. Here's a step-by-step guide to fending off trackers.

Glossary: Key tracking terminology



Web browsing activity is tracked by use of "cookies," "beacons" and "Flash cookies," small computer files or software programs installed on a user's computer by the Web pages that are visited. Some are useful. But a subset ("third party" cookies and beacons) are used by companies to track users from site to site and build a database of their online activities.

Simple Steps

Major browsers including Microsoft Corp.'s Internet Explorer, Mozilla Foundation's Firefox, Google Inc.'s Chrome and Apple Inc.'s Safari, have privacy features. To have the most privacy options, upgrade to the latest version of the browser you use.

Check and delete cookies: All popular browsers let users view and delete cookies installed on their computer. Methods vary by browser.

For instance on Internet Explorer 8 (the most widely used browser), go to the "Tools" menu, pull down to "Internet Options" and under the "General" tab there are options for deleting some or all cookies. There might be hundreds, so deleting all might be easiest. But the next time

JOURNAL COMMUNITY »

DIG DEEPER

- The Web's New Gold Mine: Your Secrets
- Personal Details Exposed Via Biggest U.S. Websites
- The Journal's Methodology
- What They Know About You
- Digits: Your Questions on Digital Privacy
- Digits: Analyzing What You Have Typed
- Digits: Lawsuit Tackles Files That 'Re-Spawn' Cookies
- Full Coverage: wsj.com/WTK

you visit a favorite site, you may need to retype passwords or other login data previously stored automatically by one of those cookies.

For guides for all major browsers, go to WSJ.com/WTK.

Adjust Browser Settings: Once you've deleted cookies, you can limit the installation of new ones. Major browsers let you accept some cookies and block others. To maintain logins and settings for sites you visit regularly, but limit tracking, block "third-party" cookies. Safari automatically does this; other browsers must be set manually.

There are downsides to blocking all cookies. If you frequent sites that require logins, you will have to log in each time you visit.

Internet Explorer lets you set rules for blocking cookies based on the policies of the cookie-placer. One option blocks cookies that don't include a privacy policy; another blocks cookies that can save your contact information without your approval. The control is under "Tools/Internet Options/Privacy."

No major browsers let you track or block beacons without installing extra software known as "plug-ins," as described under advanced steps.

Turn On "Private" Browsing: All major browsers offer a "private browsing" mode to limit cookies. Chrome calls it "Incognito." Internet Explorer calls it "InPrivate Browsing," but this option is available only in the latest version, IE8.

Private browsing doesn't block cookies. It deletes cookies each time you close the browser or turn off private browsing, effectively hiding your history.

Private browsing isn't selective. It deletes all cookies, whether useful or not. So you might want to use private browsing selectively, such as when looking at health-related information.

Monitor "Flash Cookies": Another kind of cookie uses Adobe Systems Inc.'s popular Flash program to save information on your computer. Flash is the most common way to show video online. As with regular cookies, Flash cookies can be useful for remembering preferences, such

as volume settings for videos. But marketers also can use Flash cookies to track what you do online.

To identify the Flash cookies on your computer and adjust your settings, you need to go to an Adobe website: www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html. You can delete Flash cookies stored on your computer and specify whether you want to accept future third-party Flash cookies.

The downside of blocking third-party Flash cookies: Some sites won't let you watch videos or other content.

Advanced Steps

Install Privacy "Plug-ins": Small programs called "add-ons" or "plug-ins" can help maintain privacy. Some let you monitor trackers that can't be seen through the browser; others allow you to delete cookies on a regular schedule.

Not all browsers can use all plug-ins. And some plug-ins can be tricky to set up. With those caveats, some plug-ins may be worth a look:

Abine: Developed by a Cambridge, Mass., start-up of the same name, it attempts to control several types of trackers. Once installed, the program will warn you when a site is placing cookies or Flash cookies on your machine. You can also see and block a third type of tracker called a Web "beacon" (sometimes called a "bug"). This is an invisible object embedded in a page that can interact with cookies. It's available only in "test" versions, so this is only for people who don't mind experimenting a bit with software. For Firefox, go to addons.mozilla.org/en-US/firefox/addon/11073/. For Internet Explorer, users need to request an invitation at getabine.com.

Better Privacy: This plug-in offers control over Flash cookies. It doesn't block them, but lets you set rules for deleting them—a distinction that can be helpful if you frequent sites that require you to use third-party Flash cookies to see their content. Better Privacy (available only for Firefox) is at addons.mozilla.org/en-US/firefox/addon/6623/.

Ghostery: Available at ghostery.com, it helps control beacons. It alerts you when there's a beacon on a page you're viewing, tells you who placed it and details the company's privacy policy. With Internet Explorer or Firefox, you can then block the beacon from capturing information on your computer. That feature isn't available for Chrome.

Controlling Ads

Users troubled by targeted advertising can block or limit the ads being shown. Note: These tools don't necessarily restrict tracking. Some ad networks may still collect data on your browsing

behavior and share it with others, even if you instruct them not to show you targeted ads.

The Network Advertising Initiative, an industry group of marketing companies, lets computer users opt out of targeted ads from about 50 ad networks at networkadvertising.org.

If you opt out, you won't be shown ads tied to your browsing behavior from the member networks. But you'll still see ads, which may be placed based on criteria such as your location.

PrivacyChoice LLC, an independent group, maintains a Web site (privacychoice.org/choose) that covers 152 ad networks. You can opt out of most by clicking a button there. For some, you'll need to download a plug-in, but it works only with Firefox.

Ironically, these opt-out systems work by installing a cookie on your computer. That cookie tells ad networks to stop sending targeted ads to your computer. Because these systems rely on a cookie to work, you'll need to opt out all over again any time you delete cookies from your machine.