Six Tips to Protect Your Online Search Privacy

Google, MSN Search, Yahoo!, AOL, and most other search engines collect and store records of your search queries. If these records are revealed to others, they can be embarrassing or even cause great harm. Would you want strangers to see searches that reference your online reading habits, medical history, finances, sexual orientation, or political affiliation?

Recent events highlight the danger that search logs pose. In August 2006, AOL published 650,000 users' search histories on its website.[1] Though each user's logs were only associated with a random ID number, several users' identities were readily discovered based on their search queries. For instance, the New York Times connected the logs of user No. 4417749 with 62 year-old Thelma Arnold. These records exposed, as she put it, her "whole personal life."[2]

Disclosures like AOL's are not the only threats to your privacy. Unfortunately, it may be all too easy for the government or individual litigants to subpoena your search provider and get access to your search history. For example, in January 2006, Yahoo!, AOL, and Microsoft reportedly cooperated with a broad Justice Department request for millions of search records. Although Google successfully challenged this request,[3] the lack of clarity in current law leaves your online privacy at risk.

Search companies should limit data retention and make their logging practices more transparent to the public,[4] while Congress ought to clarify and strengthen privacy protections for search data. But you should also take matters into your own hands and adopt habits that will help protect your privacy.

The Electronic Frontier Foundation has developed the following search privacy tips. They range from straightforward steps that offer a little protection to more complicated measures that offer near-complete safety. While we strongly urge users to follow all six tips, a lesser level of protection might be sufficient depending on your particular situation and willingness to accept risks to your privacy.

1. Don't put personally identifying information in your search terms (easy)

Don't search for your name, address, credit card number, social security number, or other

---

[*] By Peter Eckersley, Seth Schoen, Kevin Bankston, and Derek Slater.

[1] For more on the leak, see <http://eff.org/Privacy/AOL>.

[2] See <http://www.nytimes.com/2006/08/09/technology/09aol.html>.

[3] See <http://eff.org/Privacy/search> for documents related to Google's challenge. The logs were to be used as evidence in a case in which the government is defending the constitutionality of the Child Online Protection Act (COPA). See also <http://news.com.com/FAQ+What+does+the+Google+subpoena+mean/2100-1029_3-6029042.html> and <http://news.com.com/Judge+Google+must+give+feds+limited+access+to+records/2100-1028_3-6051257.html>.

[4] The search providers' have so far been unreasonably tight-lipped about their specific practices regarding search logging. For some insight, see <http://news.com.com/Verbatim+Search+firms+surveyed+on+privacy/2100-1025_3-6034626.html?tag=nl> and <http://www.mercurynews.com/mld/mercurynews/news/breaking_news/15315062.htm>.

personal information. These kinds of searches can create a roadmap that leads right to your doorstep. They could also expose you to identity theft and other privacy invasions.

If you want to do a "vanity search" for your own name[5] (and who isn't a little vain these days?), be sure to follow the rest of our tips or do your search on a different computer than the one you usually use for searching.

2. Don't use your ISP's search engine (easy)

Because your ISP knows who you are, it will be able to link your identity to your searches. It will also be able to link all your individual search queries into a single search history. So, if you are a Comcast broadband subscriber, for instance, you should avoid using <http://search.comcast.net>. Similarly, if you're an AOL member, do not use <http://search.aol.com> or the search box in AOL's client software.

3. Don't login to your search engine or related tools (intermediate)

Search engines sometimes give you the opportunity to create a personal account and login. In addition, many engines are affiliated with other services -- Google with Gmail and Google Chat; MSN with Hotmail and MSN Messenger; A9 with Amazon, and so on. When you log into the search engine or one of those other services, your searches can be linked to each other and to your personal account.

So, if you have accounts with services like Google GMail or Hotmail, do not search through the corresponding search engine (Google or MSN Search, respectively), especially not while logged in.

If you must use the same company's search engine and webmail (or other service), it will be significantly harder to protect your search privacy. You will need to do one of the following:

> a) Install two different web browsers to separate your search activities from your other accounts with the search provider. For example, use Mozilla Firefox for searching through Yahoo!, and Internet Explorer for Yahoo! Mail and other Yahoo! service accounts.[6] You must also follow Tip 6 for at least one of the two browsers.[7]
>
> b) For Google and its services, you can use the Mozilla Firefox web browser and the CustomizeGoogle plugin software. Go to <http://www.customizegoogle.com/> and click "Install." Restart Firefox and then select "CustomizeGoogle Options" from the "Tools" menu. Click on the "Privacy" tab and turn on "Anonymize the Google cookie UID." You must

---

[5] Or your MySpace profile, personal blog address, or other similar personal information.

[6] Advanced tip: you could also use two profiles for one browser. For instance, if you run Mozilla Firefox with the `-ProfileManager` flag, it will let you choose a profile. To learn more, visit <http://mozilla.org/support/firefox/profile>. Mozilla Seamonkey has a "Switch Profile" command in the "Tools" menu. Pick a different theme/skin for each profile so you can tell which one you are using. To learn more, visit <http://kb.mozillazine.org/Profile_Manager>. With Internet Explorer, you may need to use two separate Windows user accounts.

[7] Otherwise, your two separate browsers' activities could be linked by IP address, as discussed below.

remember to quit your browser after using GMail and before using the Google search engine.[8] In addition, be sure not to select the "remember me on this computer" option when you log into a Google service.

If you are using a browser other than Firefox, you can use the GoogleAnon bookmarklet, which you can obtain at <http://www.imilly.com/google-cookie.htm>. You will need to click on the GoogleAnon bookmarklet and quit your browser every time you finish with a Google service.

Unfortunately, we currently do not know of similar plugins for other search providers.[9]

4. Block "cookies" from your search engine (intermediate)

If you've gone through the steps above, your search history should no longer have personally identifying information all over it. However, your search engine can still link your searches together using cookies and IP addresses.[10] Tip 4 will prevent tracking through cookies, while Tips 5-6 will prevent IP-based tracking. It's best to follow Tips 3-6 together -- there is less benefit in preventing your searches from being linked together in one way if they can be linked in another.

Cookies are small chunks of information that websites can put on your computer when you visit them. Among other things, cookies enable websites to link all of your visits and activities at the site. Since cookies are stored on your computer, they can let sites track you even when you are using different Internet connections in different locations. But when you use a different computer, your cookies don't come with you.[11]

From a privacy-protection perspective, it would be best to block all cookies. However, because cookies are necessary for accessing many websites, it may be more convenient (though less privacy-protective) to allow short-lived "session" cookies. These cookies last only as long as your browser is open; therefore, if you quit your browser, re-open it, and then go back to your search engine, your search provider will not be able to connect your current searches with previous ones via your cookies.

Use the following steps to allow only "session cookies," and remember to quit your browser at

---

[8] Mail.google.com and google.com leave some additional cookies that will identify you while searching, but which CustomizeGoogle (and GoogleAnon) will not anonymize. Unless you remember to quit your browser, some of those cookies persist even if you logout of Gmail. Future versions of these privacy-protection tools may help fix this problem.

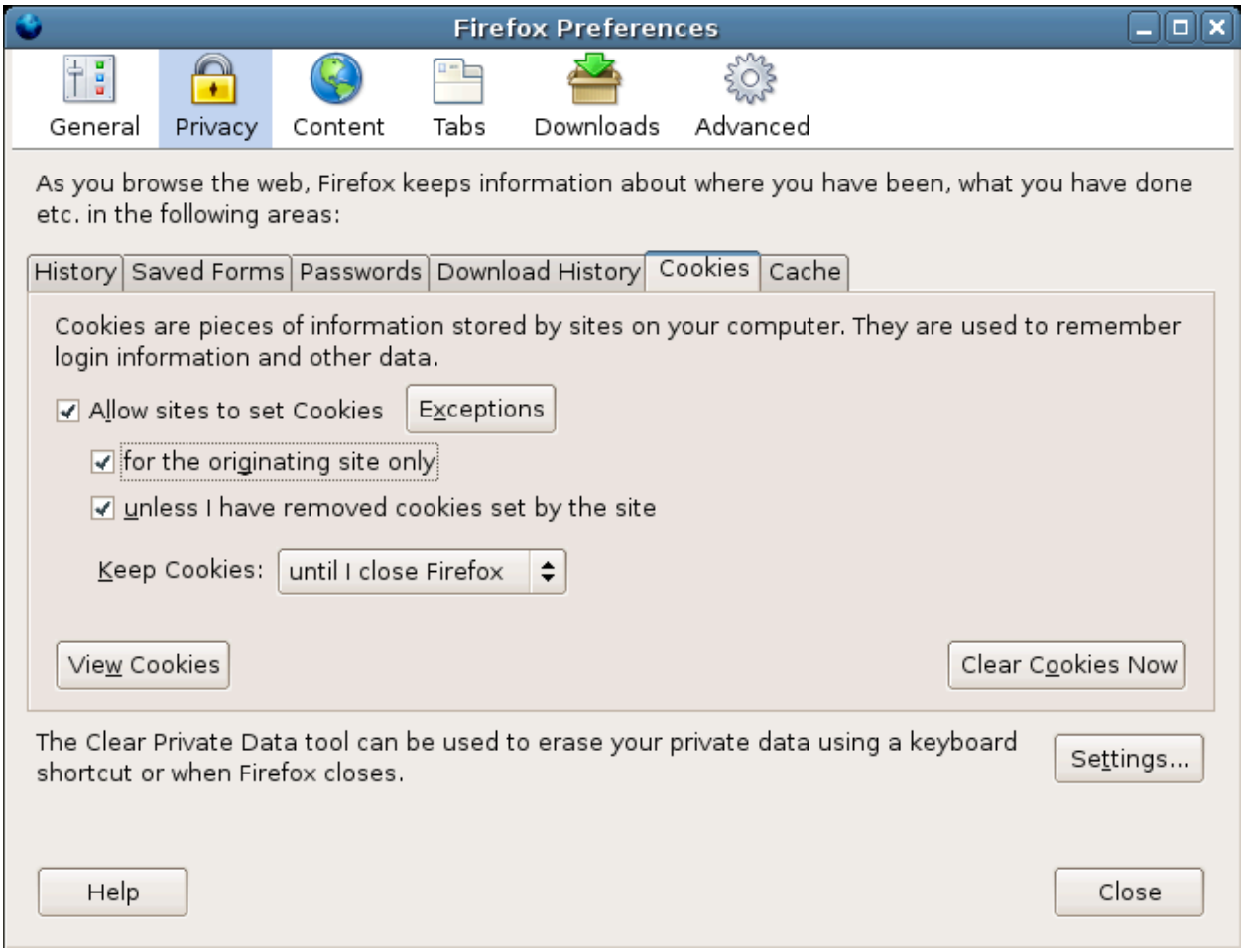
[9] There is another Firefox plugin intended to protect your search privacy called TrackMeNot (http://mrl.nyu.edu/~dhowe/trackmenot/). At present, we cannot recommend TrackMeNot. For one thing, it may actually make it easier for search engines to link your searches together (the fact that you're using the plugin is distinctive). Moreover, although it may create some uncertainty about aspects of your search history, it does not hide personally identifying information or the bulk of your most sensitive searches. For further criticisms, see <http://www.schneier.com/blog/archives/2006/08/trackmenot_1.html>.

[10] The search engine may also be able to pick you out of the crowd based on an unusual browser, operating system, language setting, or other atypical HTTP headers. The software recommended in Tip 6 can be used to impede these methods as well.

[11] So long as you haven't logged in; see Tip 3.

least once a day but ideally after each visit to your search provider's site. We recommend that you use Mozilla Firefox and apply these settings:

1. From the "Edit" menu, select "Preferences"
2. Click on "Privacy"
3. Select the "Cookies" tab
4. Set "Keep Cookies" to "until I close Firefox"[12]
5. Click on "Exceptions," type in the domains of all of your search sites, and choose "Block" for all of them

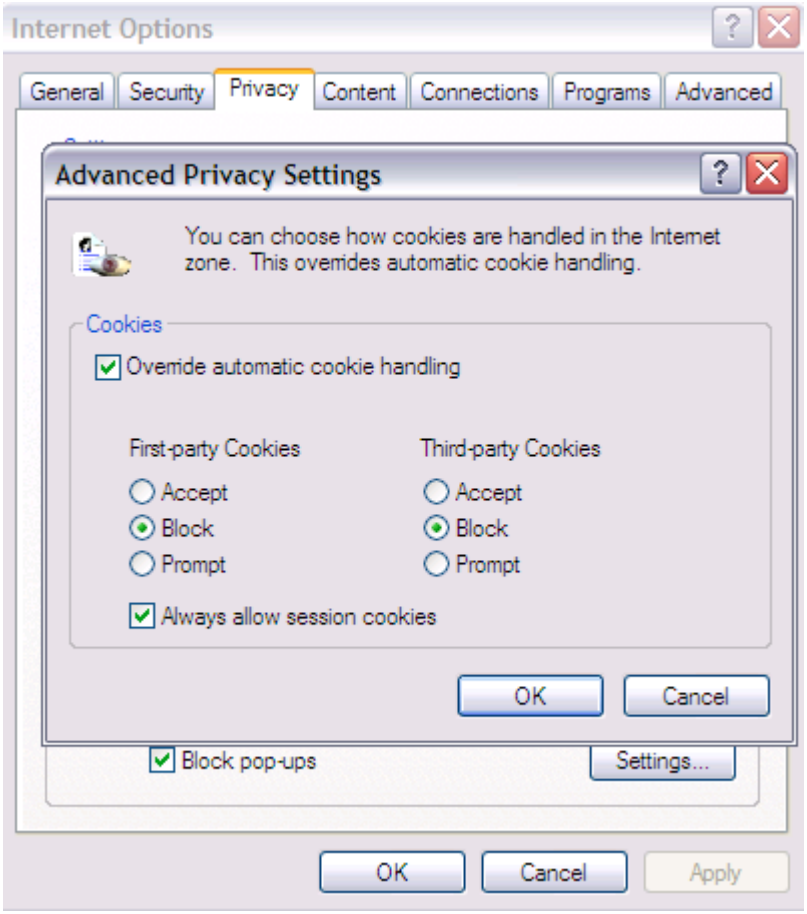


If you use Microsoft Internet Explorer to surf the web:

1. From the Internet Explorer "Tools" menu, select "Internet Options"
2. Click on the "Privacy" tab and then press the "Advanced" button
3. Click on "Override automatic cookie handling"
4. Set both "first party" and "third party" cookies to "Block"

[12] You can select "ask me every time" if you want more control, although the current Firefox user interface is not very good for this purpose. At this time, the Mozilla Seamonkey browser is more suitable if you wish to have fine-grained control over cookies.

5. Select "Always allow session cookies"



5. Vary your IP address (intermediate)

When you connect to the Internet, your ISP assigns your computer an "IP address" (for instance, EFF's web server's IP address is 72.5.169.162). Search providers -- and other services you interact with online -- can see your IP address and use that number to link together all of your searches. IP addresses are particularly sensitive because they can be directly linked to your ISP account via your ISP's logs. Unlike cookies, your IP address does not follow your computer wherever it goes; for instance, if you use your laptop at work through AT&T, it will have a different IP address than when you use it at home through Comcast.

If your ISP gives you a changing, "dynamic" IP address,[13] or you surf from an office computer that is behind the same firewall as lots of other computers, then this concern is diminished. However, if you have a dynamic IP address on a broadband connection, you will need to turn your modem off at least once per day to make the address change.

On the other hand, if you have an unchanging, "static" IP address, you will certainly need to use

[13] You can find out your IP address by visiting a site like http://www.ioerror.us/ip/. Ask your ISP if you have trouble determining whether your IP address changes.

anonymizing software to keep your address private; see Tip 6.

6. Use web proxies and anonymizing software like Tor (advanced)

To hide your IP address from the web sites you visit or the other computers you communicate with on the Internet, you can use other computers as proxies for your own -- you send your communication to the proxy; the proxy sends it to the intended recipient; and the intended recipient responds to the proxy. Finally, the proxy relays the response back to your computer. All of this sounds complicated, and it can be, but luckily there are tools available that can do this for you fairly seamlessly.

Tor (<http://tor.eff.org>) is a software product that encrypts then sends your Internet traffic through a series of randomly selected computers, thus obscuring the source and route of your requests. It allows you to communicate with another computer on the Internet without that computer, the computers in the middle, or eavesdroppers knowing where or who you are. Tor is not perfect, but it would take a sophisticated surveillance effort to thwart its protections.[14]

You also need to make sure that your messages themselves don't reveal who you are. Privoxy (<http://www.privoxy.org>) helps with this, because it strips out hidden identifying information from the messages you send to web sites. Privoxy also has the nice side benefit of blocking most advertisements and can be configured to manage cookies. (Privoxy comes bundled with Tor downloads.)

You can also use web proxies like Anonymizer's (<http://www.anonymizer.com>) Anonymous Surfing. This option is more user-friendly but possibly a less effective method of anonymizing your browsing. Anonymizer routes your web surfing traffic through their own proxy server and hides your IP address from whatever web sites you visit. However, Anonymizer itself could in principle have access to your original IP address and be able to link it to the web site you visited; therefore, that service is only as secure as Anonymizer's proxy facilities and data retention practices. While there is no reason to believe that Anonymizer looks at or reveals your information to others (we know the people currently running Anonymizer and they are good folks), there is little opportunity to verify their practices in these regards.

Using Tor and Privoxy is more secure because one untrustworthy proxy won't compromise your search privacy. On the other hand, web proxies like Anonymizer are slightly easier to use at present.

Tor and Privoxy downloads and instructions can be found here:
<http://tor.eff.org/download.html.en>

Conclusion

If you've implemented all six tips, congratulations -- you're now ready to search the Web safely. These steps don't provide bulletproof protection, but they do create a strong shield against the

[14] For a technical discussion of this subject, see <http://www.cl.cam.ac.uk/~sjm217/papers/oakland05torta.pdf>.

most common and likely means of invading your privacy via your search history.