From: http://www.abine.com/

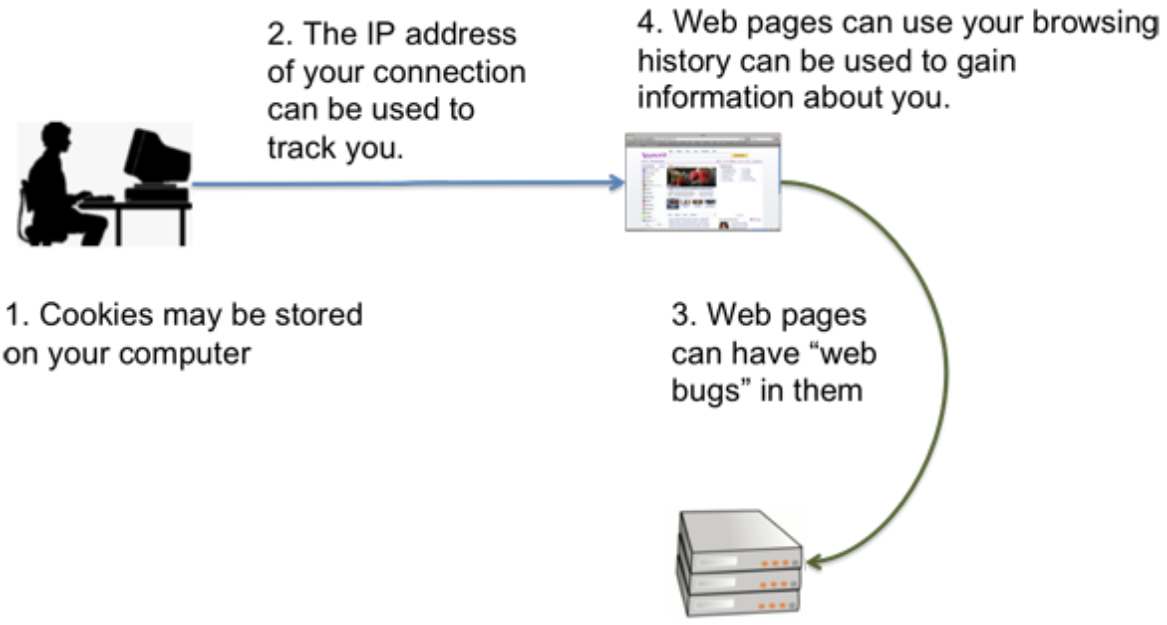
How you can be tracked online

Most of us don't realize how easy it is for our online behavior to be tracked. ISPs, websites, and advertising networks all have ways of tracking your online behavior. They track you to provide targeted advertising, classify you into a demographic group, and resell information about you to other companies.

Similar to mail-order catalog companies that sell and re-sell your name, address, and phone number to others trying to sell you related products (the beloved "junk mail" in your home mailbox and telemarketing calls to your home phone), so can website and advertising networks sell the information they gather about you to other advertisers and private companies.

But unlike the catalog company that knows only very basic information about you, a website potentially knows much more. Websites do their tracking by looking at cookies, IP addresses, web Bugs, and your browsing history, among other techniques.

The four main ways that you are being tracked online:



1. Cookies

What are cookies?

Cookies are small pieces of data that websites can store on your computer. This is the most direct way of tracking your behavior. A website can "tag" your computer with a cookie, which identifies you as a unique visitor to the site. When you visit the site again later, the website can read the value of this cookie that's stored on your computer to identify you and know that you are visiting again. This means that every time you visit that site, they know it’s you.

Cookies can be used to help websites calculate how many visitors they have, customize the content of their site depending on the viewer, and assemble convenient tools, like online shopping carts and checkout options.

But because cookies are stored on your computer, anyone with access to your computer can use cookies to see which sites you've visited in the past. In some cases, they can even access websites as "you."

There are four types of cookies:

1. **HTTP Cookies**. These cookies come from the website you're visiting and are usually intended to stay on your computer permanently. We recommend that you delete all HTTP cookies at the end of each browser session.

2. **"Session" Cookies**. These cookies are the same as HTTP cookies, except that while HTTP cookies are intended to be permanent, session cookies expire when you close your browser. Some sites, such as Gmail, require the use of cookies during a session in order to function properly, but they don't need to have cookies stored permanently on your computer. Unlike with HTTP cookies, we recommend that you allow session cookies in order to avoid breaking functionality on certain websites.

3. **Third Party Cookies**. Web pages often have pieces of content from more than one source (such as ads posted along the sidebar of a page you're viewing). Domains *other* than the main page you are viewing (third parties) set these cookies. In most cases, advertisers use third party cookies to track users across multiple websites. We recommend that you block third party cookies.

4. **Flash cookies**. Unlike the 3 types of cookies described above, which are controlled through the cookie & privacy controls in your Web browser, Flash cookies are activated through a feature in Adobe's Flash plug-in called "Local Shared Objects" (LSOs). This means that even if users have cleared their cookie settings (by directing their browser to "block" or "delete" cookies), sites can still use a feature of Flash to track their online behavior. Among other things, Flash cookies are used to ensure smooth playback on sites that stream music and video. Abine recommends that you delete all Flash LSOs at the end of each browser session. Note that this is not done the way other cookies are deleted; instead, a user must visit Adobe's site for the deletion controls or use other software such as Abine's Privacy Suite.

How are cookies used to track me?

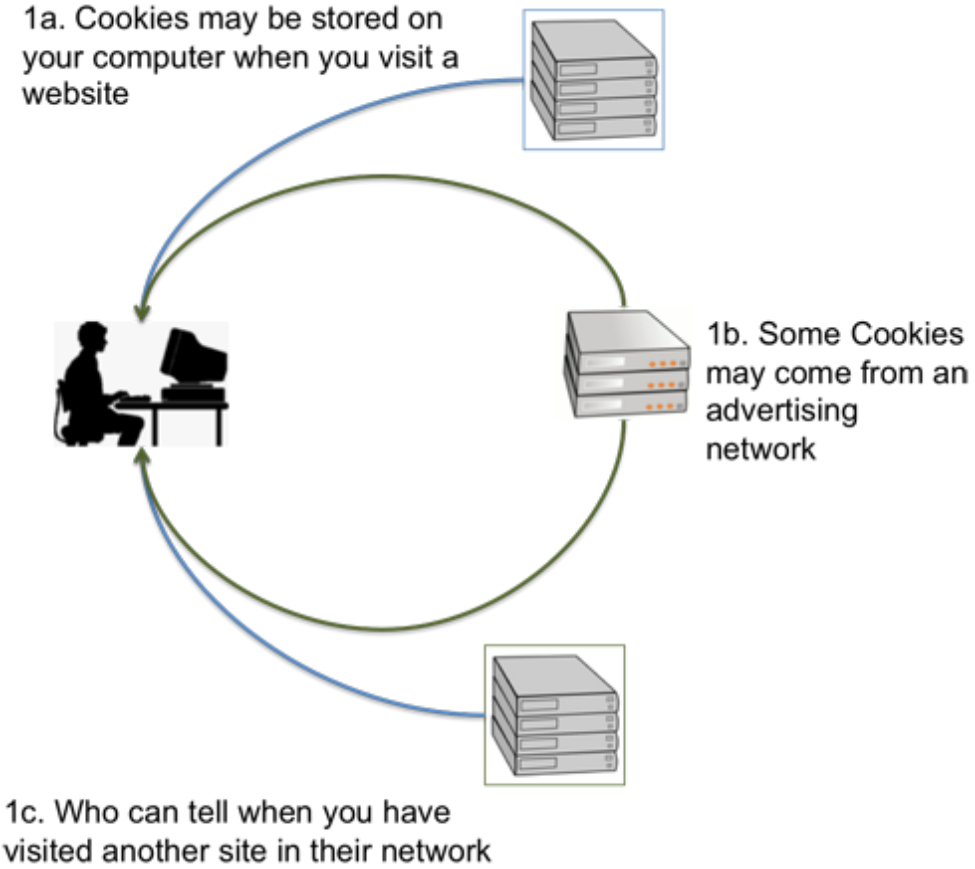
Cookies left on your computer generally store, among other things, a unique serial number that can be used to identify you and to keep track of all your visits to a particular website and any "network" of sister sites.

If you allow third party cookies be stored on your computer, then each time you visit a website in the cookie's "network," the network (generally an advertising company) can track you as you travel among these different sites.

Advertisers can then create a profile of you based on your browsing behavior, as well as store your browsing history as long as they like.

If you're interested, you can read more about cookies at Wikipedia.

Abine recommends allowing only session cookies and blocking third party cookies.



2. IP Address

Websites that you interact with always receive your computer's current IP address -- it's how they know where to send the webpage content you've requested. With your IP address, websites can 1) determine your geographic location down to the level of your zip code, and 2) keep track of all connections from the same IP address. If your IP address doesn't change, then they have a good idea that it's you every time you visit. You may have a dynamically-assigned IP-address if you use a cable modem, but these tend not to change very often. Most other forms of internet access use static, or unchanging, IP addresses.

To prevent websites from discovering your geographic location and tracking your repeated visits, you must direct your internet traffic through different IP addresses. You can accomplish this through free or paid proxy services, which act as a courier between you and the websites you visit, forwarding traffic back and forth without revealing your IP address. In these cases, the website sees only the IP address of the proxy server. (Note that the proxy servers *do* see all of your traffic.)

Abine recommends using a proxy server if you require high levels of privacy. Free proxys are too slow, and there is usually a cost for fast proxy servers.

3. Web Bugs

What are Web bugs?

"Web bugs," also called "beacons", are objects, usually invisible to the web page viewer, that are embedded into a website's HTML to track who is viewing the page, at what time, and from what IP address. While there are several species of Web bugs, their basic role is to do things like monitor a customer's activity on a website and report whether an email was read or forwarded. Web bugs can see that your machine made a request from one site and traveled to another; they can track you as you move among websites within their network.

Abine recommends blocking all known Web bugs. Here are some of the ways this is done:

1. **JavaScript trackers**. These are pieces of JavaScript, a computer scripting language, that usually come from other sites. When the Web page loads in your browser, it makes a request to include a piece of code from the tracking server.

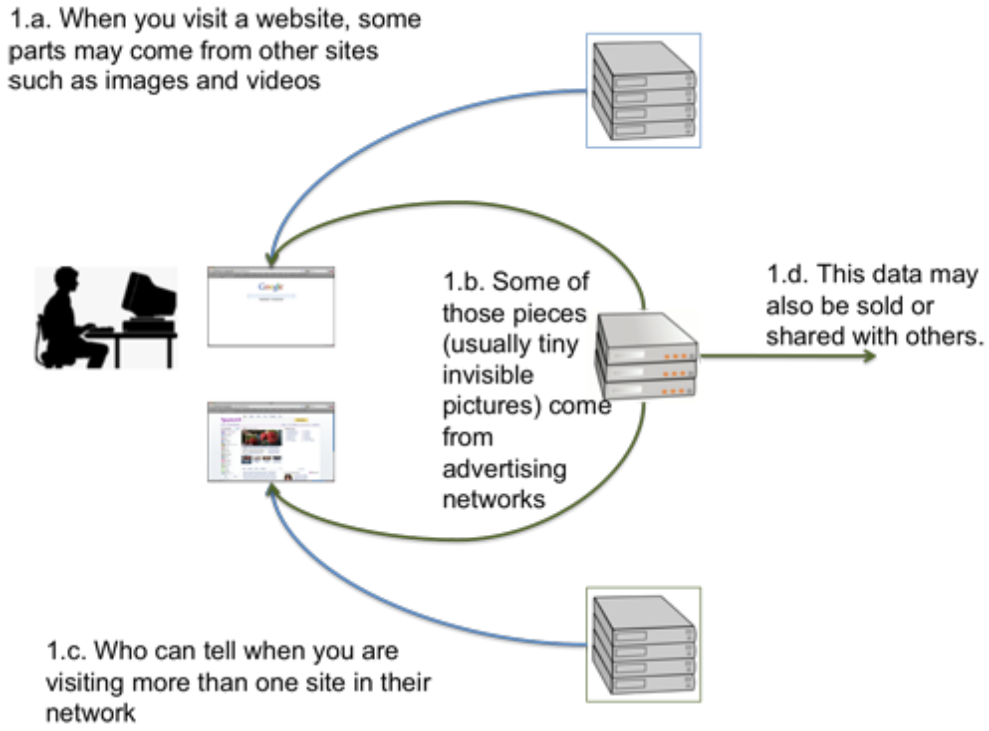
2. **One-pixel images and other SRC tags**. Image tags in HTML pages are actually directions that tell your browser where to find the image it is supposed to display to you. This means that when your browser displays a Web page to you, it makes a request to the tracking server for the image. Usually the image is a transparent 1-pixel image, i.e., it isn't really meant to be viewed, and it's just a tracking method.

3. **Browser fingerprinting**. It is also possible to identify a specific browser by directly examining details about its software and components. We are not aware whether websites currently use this technique, as it is a less convenient tracking method, but it does represent the next frontier in online privacy. Visit IP address above).

Advertisers can then correlate your visits to their sites by looking at the timestamps of the requests from the Web bugs you triggered, and use your IP addresses and browsing sessions on their sites to build up their profile. Note

that Web bugs can be in anything that renders HTML, such as HTML emails, so they can tell if you've opened their email and where you were when you opened it.

Abine recommends blocking all Web bugs.



4. Browser History

Websites can also look at your browsing history through JavaScript or a Cascading Style Sheet (CSS) technique to see portions of your browsing history.

To do this, the website maintains a list of all of the sites it is interested in, and if you are keeping a browsing history, it can learn whether you have visited those target sites in the past.

Advertising groups sometimes use this to put you into a demographic bucket (e.g., did you visit sites about guns, cars, and girls, or sites about Disney, toys, and motherhood). For an example of this technique, visit here.

Update: FireFox v. 3.5 or later addresses most known CSS history sniffing techniques.

Abine recommends not keeping browsing history.