Going Incognito: 4 ways to limit being tracked online

Author : Cat

Date : June 18, 2015

Every time you go online you add to your digital footprint, or binary tattoo. The information collected is made up of *what you enter online* (likes, comments, posts), *your behaviour* (what sites you visit, how you interact with them) and what *inferences companies can make* based on the first two pieces of data. This data is used to target ads and make marketing decisions.

The actions of what you enter are easy to correlate and make assumptions on. If a large sampling of 15 yr olds that like *Game of Thrones* and *Marvel* comics are found to also like *Star Wars*, then advertisers will be sure to show *Star Wars* ads to all the teens that fit the profile of the first two - with probable success. What is interesting is how advertisers are also able to use browsing history and actions. For instance, what if lots of people watched the trailers for *Fifty Shades of Grey* but no one ever 'likes' the movie. This could indicate that this audience was interested in the movie but perhaps didn't want to publicly declare it. That may help in targeting the sale of DVDs or books to those that watched the trailer.
Websites pass this information around using various devices and systems. If you do not like the thought of Trip Advisor having your Facebook friend list or of Amazon knowing what you watched on YouTube, here are a few suggestions to tighten up how much information you give away:

1. Cookie Control

A decade ago people thought cookies were just yummy treats. Now it is becoming commonplace to talk about cookies as files of information about you that are passed from website to website. When you visit a site, that site may set up a cookie that lists things like preferences, login information and

history on that page. Have you ever been shopping online, left the website and then returned to find your 'cart' still full of the right items? That's cookies at work. Typically the cookie is created by the site and used by the same site so it is very useful. Sometimes though, those cookies can be shared from one site to another.
As an example, Facebook assigns you an ID which is listed in your cookie. When you visit a secondary website that works with Facebook, they can read your ID from your cookie and show you information related to the public information available like your profile photo. Here's where it gets sneakier. Let's say your friend list is private BUT one of your friends, Bill, has a public list. Bill visits Trip Advisor. Trip Advisor reads Bill's cookie and notes all the IDs of Bill's connections. Now when you visit Trip Advisor, the site reads your cookie and matches the ID up to the list of Bill's friends. It will then show you Bill's picture as someone you know who was been to the site... even though your privacy settings are locked down.
Want help managing your cookies? Here is a great resource for controlling your cookies, listed by browser.

2. Logging Out and Single Sign-on

To stop the cookies from tracking you, the easiest thing you can do is log out of a service when you are done using it. That means actually signing out, not just closing a tab. Cookies are not allowed to persist when you have logged out but they are allowed to be used when you remain signed in. If you have a gmail account and open YouTube, check to see if YouTube already knows who you are. If it does, it is because you have not logged out.
Another way companies are tracking you is by Single Sign-On, or SSO. This is when a website presents you with the option to use an alternate sign in (Twitter, LinkedIn, Facebook etc) instead of creating a new account on their site. SSO is becoming much more popular and Social Networks make them easy to use. The issue with SSO is that you give away loads of information each time you use it, even if that data is protected. For all the details, check out this post I wrote on the information you give away when you use SSO.

3. Private Browsing

While you are browsing, your browser keeps track of all the sites you have visited, what you have downloaded and what you have searched. This is called your browser history. It also remembers certain things like your email address or home address so it can offer to automatically fill this information in when you need it. If you do not want your browser to maintain this information you can use Private Browsing, or Incognito mode. This is especially useful (and recommended) when you are using a computer that could be used by someone else. Each browser varies slightly in what they don't track and in how to set it up. Check out this resource on using private browsing with your browser.

4. VPNs

If you want an additional level of security, you also have the option of a Virtual Private Network, or VPN. A VPN encrypts your data in a way that no one can intercept it and read it. Sensitive data being sent through a public WiFi connection could be made safe by using a VPN. Much like remote employees use it for access to company servers, you can also use it to connect in to your home computer from outside your house and know that the connection is secure. For our purposes, VPNs also mask your IP address which means when you access a site, that site does not have your geographical information nor can it track you by the machine you are using. There are many paid services that will set up a Private VPN for you. Here are the top 10 services evaluated by PC Magazine.

No matter what level of privacy and security you decide to use, take the time to understand what information you give away when online and make sure that you are comfortable with it.