When I say that you're tracked online I mean that a lot of things that you do when you are using the web is tracked, saved and used by big companies to make money. I will talk about a few ways in which information about your behavior online is valuable and how it finds its way into the hands of who is interested in it. The fact that you are being tracked is problematic when sensitive information is disclosed to parties who were not supposed to have that information. An example of disclosed information is when you want to surprise your partner with a vacation and the surprise is ruined because commercials for the destination you searched for is shown on a lot of online advertisements. Another example is when insurance companies heighten your yearly fee, because you've been searching for AIDS related topics.

You may think that this kind of disclose doesn't apply to you or is not so bad and that you don't have anything to hide. While this is probably true you can ask yourself whether your friends and family are in the same position and whether you may be in need of privacy as you get older for instance and your medical data becomes more valuable to insurance companies. I hope you come to the same conclusion as me and find that we are better off in a society where we don't have to worry about whether sensitive information gets revealed or not.

I could sum up a set of incentives which would protect your privacy and stop writing this essay. In fact I have made this list here for anybody who doesn't want to read further than this. However a rule without an explanation of why that rule is important is just another rule and such rules are likely to get broken. That's why I want to explain you in simple terms why these rules are important and how they affect your privacy. It will take a little more effort to understand the essay than to read the bullet point list of incentives, but you are more likely to remember and follow rules once you understand their reason. Once you know these rules you can not only protect yourself but also people who are in greater need for it and haven't red this essay themselves.

A website is a collection of webpages. It's best to picture webpages to be some kind of PowerPoint slides. This metaphor for what a webpage is works well, because like a Power Point slide a webpage can change when somebody interacts with it, for instance when you click somewhere, or automatically when some sort of timer is in place. A difference between a PowerPoint slide and webpage is that any changes always become visible, while on a webpage this is not necessarily the case. In fact tracking is for a significant part done by changing the webpage invisibly when you are looking at it!

When you visit a webpage on a website you're using a computer program that is called a browser. Examples of browsers are Internet Explorer, Firefox, Chrome, Safari and Opera. As soon as you click on a link somewhere your browser makes connection with a computer which stands in a room like you see below:

Many powerful computers are stored in those things that look like fancy refrigerators on the image. When you see a webpage in your browser it has been send to your browser by one of these computers.

However there is a catch to this that is important for the way that you're being tracked. Your browser receives an entire webpage in parts. The first part, which usually contains all text on the webpage, will also indicate to a browser where it can find other parts. These parts may be images, video or audio that are on the webpage you're visiting. Since these parts are often essential to the look of the webpage your browser will download these parts without checking if they are necessary. These additional media parts could be located on the same computer as the webpage your visiting, but they could also be present on computers which are in a room on the other side of the world as the computer that gives your browser the webpage. A website logo is often retrieved from the same computer as the first part of any webpage which is part of that website. However some images are almost never on the same computer as the webpage, that shows those images. Think for instance about Facebooks “like it” buttons or Youtubes video players, but also banners and commercials. These media are retrieved from Facebook, Google or another media company. When that happens the computers, from these companies, not only provide the requested media, but also record that you have received the media when visiting a particular webpage from a particular website.

Now the question remains how these 3rd party computers (computers other than the computer delivering the main part of the webpage) know that it is you who is visiting the webpage. Lets make clear that in principle you reveal as much about yourself to a 3rd party computer than to the computer who serves you the main part of a webpage.

Whenever you are asking for a part of a webpage your browser tells a few things to the computer that is supposed to deliver that part to you. It depends on the browser what gets told exactly, but usually it will tell which browser you are using and if you are on a Mac, Windows, Android or other kind of computer. It may also reveal your language setting and which webpage you were visiting before. This information combined already tells a lot about you, because only a few people will send exactly the same information. This makes you identifiable. The really revealing information that gets collected however is the IP address in combination with the content of a so called cookie file.

When your browser connects to a computer for a part of a webpage this computer does need to know where to send the part of the webpage to. To inform websites where you want the webpage parts to be delivered your browser specifies your IP address (Internet Protocol Address). Sometimes you share this address with the people you live with and it can also happen that you get a partially new address every time you turn on your computer (depends on your internet provider). In general the IP address will limit the size of the group of people who may have asked for the webpage significantly and thus comes very close to identifying you.

The identification is further completed by the use of cookies. Cookies are files that are stored by your browser when you are visiting websites. The content of these files is determined by the computers who send you the parts of a website. So the computers not only send the media or other kind of webpage part you're interested in, but also what the computers want your browser to store in a cookie file. Your browser obeys by default. Whenever you ask again for something from the website, your browser will not only request for the webpage parts, but also remember the website computers what was stored in the cookie file. The content of a cookie file might be the products you’ve been shopping for so far on a certain website for instance. When you visit the paying webpage the content of the cookie file gets transferred to the website. In this case a correct bill may be generated from this information, since it contains all products you shopped for, which is then shown on the webpage you asked for.

So far so good, but what if a website stores something like a social security number inside a cookie? In that case this identifying number gets send over to the website every time you visit a webpage from that site or download a webpage part from that site. Such numbers stored in cookie files may uniquely identify a user on a wide range of different sites and this happens for example with Facebooks “like this” buttons.

Your FacebookID, which is stored in a cookie, gets send over to Facebook whenever you visit a page with such a button. This happens because your browser will always send any information present in a cookie file to a website where want to download something from. Even when it's something as trivial as a like button. Remember that a lot of webpages have “like it” buttons even when they are not really part of Facebook. In those cases the button part is separately retrieved from a computer owned by Facebook and not the website you were originally visiting. Since every request for a webpage part that needs to be collected from Facebook will be done with your browser sending the information in your Facebook cookie file back to Facebook, the unique number tells Facebook exactly who you are. Whether you're on Facebook or some other site that has a Facebook button on it doesn't matter.

You don’t even need to be signed in to a platform for this cookie trick to work. All it takes is that a 3rd party computer generates a big unique number for you ones. When this is stored in a cookie the website computers can relate all different requests for website parts with each other. They'll now what you've been doing on internet and can then adjust what they send back accordingly. How companies make profits by knowing who you are will be subject to the next part of the essay.