How It's Collected

Data collection is not that hard of a concept as many might think it is. In fact, it is often the user giving away their data. Below are two instances of data collection:

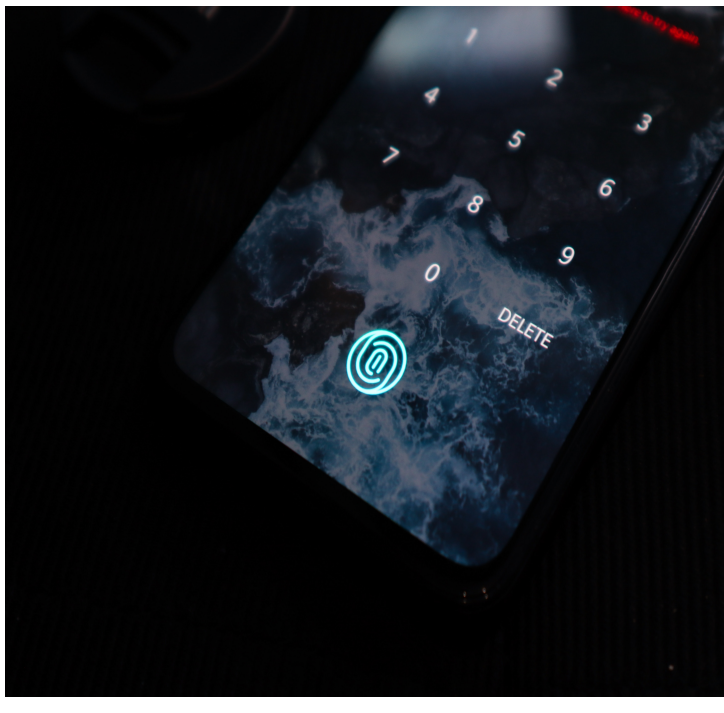
How Facebook Collects Your Data

Facebook itself asks you for a lot of you personal information. You give them a lot of basic information such as full name and birth dates. The issue is when you give them the extra information such as your hometown or phone number. This information is not out there on the internet and in the hands of Facebook as well.

Facebook also collects other information about you from your likes and viewing history. All of the pages you like help build the advertisement persona that businesses seek. In tandem with all of the information you already give Facebook, they have a wealth of personal data on you that they keep collecting to turn a profit. This profit led to them collecting as much information as possible. They have the potential to tell you your favorite shopping stores, your location, and possibly even your typical driving routes.

Fingerprinting

A new problem many privacy experts are alerting masses about is the browser fingerprint. A browser fingerprint is the term used to refer to the trace that your exact web browser is leaving behind. This trail left behind can leave information about yourself, more specifically your web browser itself, discoverable to others. All of this information is collected through Javascript. Javascript requires a lot of information about your computer system to run properly, which is why it can be so dangerous to use unprotected. These fingerprints can let third parties know what web browser you are using, the operating system, the screen resolution, the default language, the time zone, active web extensions- a lot of your information.



There are a number of ways to counter browser fingerprinting. One way is to change the browser you are using to something more secure, such as Firefox 72 or Tor. Firefox 72 was released in January 2020 and has features to specifically block fingerprinting, and Tor Browser itself is already a very secure and discrete browser. To ensure that these browsers stop fingerprinting, make sure to turn off Javascript entirely, especially if using Tor. Javascript is how these traces are left behind, so turning it off entirely will greatly aid your cause.

A big part of stopping fingerprinting is being aware of it. Not enough people are aware of fingerprinting at the moment, which makes it that much more dangerous. A good idea would be to tell your friends and family about its potential dangers in order to potentially save them in the future.