# Permissions & Settings

Permissions! Like giving the permission to access your data is something very powerful that we typically overlook. We tend not to read the permissions we grant services, and we unknowingly configure our operating systems to allow ourselves to be tracked. This is obviously a big problem for several reasons. Let's cover some stories and scenarios where permissions led to privacy invasions, and how we can change that!

*After you have my permission to continue watching after this short message...*

## *Promotional Spot*

Recently, Facebook suffered a pretty big hit after it was revealed that a company called *Cambridge Analytica was stealing private customer data from users who authorized access to their Facebook account.* This was HUGE, millions of people's information was stolen and it's *believed to have been used to influence the 2016 US election.* On top of that, *Facebook tried to push it under the mat until it was finally made public.*

*Android typically enables location history, which tracks everything you do and everywhere you go with extreme accuracy. You can open your Google maps and view the timeline of your entire life if you haven't disabled this yet. Apple does the same thing with their significant locations setting, comboed with Popular near me, device analytics, and more.*

Uber is an app that routinely asks users for permissions, including access to their location, *something that's necessary to use the app in order to find drivers.* Uber compiles a personal collection of every trip users take, creating a digital honeypot. *A honeypot is a large amount of wanted information in one easy-to-access place, which can be easily targeted by hackers or other data collectors. In 2015, Uber changed some of its privacy policies so that they could collect location data from all US-based users when the app was running in the background, even if the satellite and cellular communications were turned off. By using nearby Wifi and IP addresses.* This titled 'god view' was extremely dangerous and unneeded, since it collects data about everywhere you go when the app isn't even open. *Additionally, Uber also got caught for working with Apple on a secret permission allowing them to copy a user's screen content.*

On the topic of cars...Tesla is an excellent company that makes phenomenal cars. *When you buy a Tesla, you're given a consent form which gives you the ability to allow Tesla to record any information about your car over a wireless*

*communication system. If you accept, Tesla will collect your Vehicle ID, speed information, odometer readings, battery usage information, battery charging history, safety-related data, and much more*. An entire portfolio of where and how you drive is created which you have no control over, Tesla owns it and can do with it whatever they please. You can contact Tesla to opt out of this, but you will miss out on automatic software updates, as well as other features of the car.

The lesson with all of these stories is the less permissions you grant programs and apps the better. *All it takes is one of these companies to suffer a breach for your information to be publicly available online*. Practice minimalism to avoid rogue permission abusers, *go through all the settings on your devices and deny any unneeded permissions, and restrict as many features and settings as possible, especially unneeded ones*. You have to remember that by default, most companies will heavily track you. It's up to you the user to take back ownership of your data.

Some good pointers:

- *Don't enable information sharing between apps.*
- *Disable diagnostics and other information sent to the manufacturer of your device.*
- Find alternatives to apps, programs, and services you use that are FOSS and non-proprietary.
- Personalization is the enemy, so make sure to disable as many settings and app permissions that can be used for personalization, because personalization is a synonym for data collection.
- For Android devices, checkout the Appcensus website, they break down privacy concerns for lots of apps from the Play Store, so it may be worth checking this before downloading an app.
- As we'll discuss later, ditching Windows 10 isn't a bad idea, it's a privacy nightmare, but for many of you--you may still need to use it. *You can optimize windows 10 for privacy and security, using tools like these, although keep in mind they don't remove 100% of everything, they just help.*
- Avoid syncing accounts that allow friends or family members to access or share private information. It's easy to end up in a situation where you have to *explain to your kid what's that monster hanging between your legs and why their mother sent a salivating emoji as a response to it.* Try to keep your accounts private, and only accessible by you to avoid any possible confusion.
- Lastly, make sure you're the administrator and that any other users or guests have limited permissions. This is similar to the principle of "least privilege" in a corporate or security setting. Where employees are granted the minimum permissions needed to get a job done.

## *Queue Outro Promos*

I hope that helped you understand the need for limiting permissions, because most data breaches and privacy invasions are a result of poor permission etiquette. It's important for you to understand what type of data is being collected about you from the features, settings, apps, and programs you use everyday. Remember minimalism and transfer the ideas from there to here. Thanks for watching, and I'll see you in the next lesson talking about *passwords.*