Why Google Is Evil

and what you can do about it.

At first, Google seems like the perfect company. They offer hundreds of services, all for free, with minimal ads. Ads alone don't make enough money to keep Google running, so how do they do it? By collecting, selling, and using your data.

You've probably heard about this before, and had some time to think about it. Chances are you avoid giving out your personal information online. However, this doesn't protect you at all from the biggest problem, the information collected that you don't know about.

A common argument against people who are for the protection of privacy is that, "I have nothing to hide!". Do you have passwords you like to keep secure? Credit cards? If so, then you have something to hide. Even if you are the perfect person, and you never make any mistakes, or do anything morally questionable or against the law, you still have stuff to hide!

What does Google know about you? Way more than you think. Most people think that Google only knows what you search, but there's so much more. Google knows who you've emailed, and what those emails said. They know what you've bought, where you've been, who you know, your passwords, your devices, and even your grades if you're a student! Don't believe me? Here's a list of Google services along with the information they have about you.

1. Google Maps – Knows where you've been, and where you are. Depending on the phone brand you use, they can even tell where you are when you have the app closed.
2. Gmail – Knows who you've contacted, when, and for what reason.

3. Google Shopping – Knows what you've bought, what you're interested in buying, and things you've recommended to friends and family.
4. Google Contacts – Knows who you know, how you know them, and all their personal information that you've entered in. Even if you haven't entered their information, the app on your phone might have automatically taken their information from your native contacts app if you allowed it to in settings.
5. Google Chrome – Knows all of your passwords that you've saved, along with your entire browser history or cookies. Google Chrome also has access to your location, microphone, camera, files, and other data on your device.
6. Google Classroom – Knows all of your teachers, where you go to school, what your grades are, what assignments you've had, and who you go to school with.

Google has stopped at nothing to make sure you can't stop them from accessing your personal information. Consider this:
1. Google started by creating their own **search engine**, which they used to track user information. However, as other search engines arose, Google lost the ability to track users as they used other search options.
2. To solve this, Google created their own **browser** 'Chrome'. This way, they could track users anywhere on the internet, even if they didn't use Google as their default search engine. However, as other browsers started to gain popularity, that had to come up with another solution to track users even if they didn't use Google Chrome.
3. To solve this new problem, Google created their own **operating systems**: Android and ChromeOS. This allowed them to track their users no matter what search engine or browser they used. However, tech savvy users began installing their own operating systems in order to increase their privacy.
4. To solve this, Google created their own **devices**: The Google Pixel, Google Home, etc.". These new devices allowed Google to track users no matter what search engine, browser, or even operating system that the user decides to use!

Imaging if this process keeps on going. What if Google begins to implement **city infrastructure** in order to help support new devices? This proposal may sound crazy at first, but actually think about it. This would allow them to track users no matter what search engine, browser, operating system, or device they use. In other words, Google would be able to track you no matter what you do. You may also think that this is impossible to pull of, due to current laws set in place. What about the self driving vehicle technology Google is developing? Implementing city infrastructure to help guide these cars seems like a fairly reasonable proposal that many people would be fine with.

So what can you do about it?

Avoiding Google is not as hard as it may seems. You don't necessarily have to stop using their services entirely. What makes Google dangerous is that they have all of your information in one place. All services have some degree of your personal information, it's simply the magnitude of it that Google has that you should worry about.

A good place to start is by using a different search engine. DuckDuckGo is a great choice. Its free, just like Google, and many of the features you see on Google today were actually created on DuckDuckGo first! DuckDuckGo's entire business strategy is that they don't track you in any way. This is ideal for privacy for obvious reasons. While this will only really help if you use a browser that doesn't track you, it's a good place to start.

DuckDuckGo: duckduckgo.com

The second thing you should consider is using a different browser. The two I'd recommend are [Brave](#) and [Firefox](#). If you're just a normal internet user, Firefox should work just fine for you. Brave, on the other hand, is for the users who would like full control over their online security and privacy. It's more difficult to use, but not to the point where a non-tech savvy user would struggle to use it. If you want to go all out, then [TorBrowser](#) will give you nearly infinite privacy. However, TorBrowser is much more difficult to use, and most websites won't even load properly using it. TorBrowser routes your internet connect through a handful of 'nodes' before connecting you to the internet. This means that you are nearly untraceable, even to the websites you visit. All the browsers I have listed here are open source, which means anyone, including you, can examine the code to ensure they are safe to use. Please note that the link for Brave is a referral link. However, I would recommend this browser either way. I strongly believe it is one of the best browsers available today, and that it offers the perfect balance of privacy and usability. If you don't wish to download Brave without using my referral link, simply visit [here](#) instead.

Firefox: https://www.mozilla.org/en-US/firefox/new/
Brave: https://brave.com/cvp545
TorBrowser: https://torproject.org

The third, and most intensive thing you might want to consider is getting a more secure device. For a cell phone, I would suggest the iPhone from Apple. While there have been some security problems in the past, it has one of the best security and privacy reputations of any mainstream smart phone. It definitely isn't perfect, but if offers a good balance of security and usability. For a secure computer, I would suggest a Mac. Macs have a reputation for being secure and for protecting your personal information. However, MacOS is not open source, so if you'd like to protect your personal information even more, that you might want to consider installing Linux. Although Linux is much more difficult to use, it's much more secure. Between MacOS, Windows, and ChromeOS however, MacOS would be the clear privacy leader.