# Privacy is a fundamental right – but not on the Internet

The Internet is a network, and by default, you are connecting to other network points when you go online. The exchange of information over the Internet created unprecedented growth for the economy, among other things. Still, the development of social media, smartphone applications and other services started a grey area where users' privacy is endangered.

Once smartphones came into the hands of the vast majority of people, a new era of tracking began. Many apps use location services to provide a better user experience. However, collecting data opens up a side job that involves marketers who can create customized and better-targeted ads with precise user data.

## How websites and apps invade privacy

To protect yourself from privacy intrusions, you can use numerous tools. VPN services, proxy servers or specialized apps for spoofing locations are some options. Using a proxy server is the easiest way to hide your IP address, but before you start, make sure you use a proxy checker to see which service offers the best experience. Not all proxies are the same and using free services can create more damage. One of the tools you can use to test the proxy server is<https://proxyway.com/tools/free-online-proxy-checker> so that you don't go with subpar providers.

Why do you need a proxy server? Have you ever looked for new sunglasses online or any other product? Did you notice ads on other websites aggressively started offering you various glasses in the next few days or weeks? Suppose you don't examine privacy settings on a web page and automatically accept all the cookies. In that case, you will fully give your data to the site and subsequently to thousands of marketing agencies that use those data. In some countries, you can see the list of companies that use your browsing data.

## It gets worse with social media

Websites are not the only party that gets your data and sells it afterwards. Mobile apps for weather forecasts, Netflix and others also aggregate as much data as possible and then transfer it to third parties. Apps can collect each and every step you take and create a unique pattern of your behaviour that can't be replicated. For example, your digital fingerprint is so different that someone can identify you within a minute.

For now, most applications are focused on the marketing part of your user behaviour but being paranoid about privacy and anonymity is not so crazy because it is a matter of time before someone will misuse the gathered data.

All this [data gathering](https://en.wikipedia.org/wiki/Data_collection) is perfectly legal. The European Union made huge strides trying to impose a GDPR directive that tackles privacy data. The USA and the rest of the world don't have such restrictive laws. But even in Europe, websites and apps can and do collect your private data if you click allow.

A social media giant Facebook is notorious for breaching privacy. Social networks collect data while you use the app, but it also uses data from third-party apps while you are not using it to create a more authentic marketing experience. After immense pressure, Facebook had to implement a new Off-Facebook Activity menu that allows you to delete your private data.

## No need for Big Brother

If you ever get scared of the government that follows you, or a secret organization, you should know they don't have to invest in tracking you. Chances are, you have will fully exposed your identity and continue to build on your online database by using various apps, shopping online or reading articles on news outlets.

With our smartphones and online profiles, location services, and Google ads, you can easily be recognized, monitored, and exposed. There is no need for expensive surveillance equipment or spies. Everything is a few clicks away.

## How can proxy help?

If you selected a viable proxy server that checks all the boxes from the proxy checker, you could use it to hide your IP address. Proxy is another computer in a nutshell, and you send your data packages to a proxy, which then interacts with the network. Internet response comes to the proxy and then filtered back to you.

Using a proxy server, you will hide your [IP address](https://en.wikipedia.org/wiki/IP_address), increase the level of anonymity and create a more secure buffer zone between your client device and the Internet. However, all these features are not dependable if you choose an accessible proxy server. Instead of protecting your privacy, free providers have oversaturated websites with ads. Malware and user tracking are also common with free proxies. A proxy checker can help determine which provider has quality service.

## Bottom line

If you care about privacy, there are numerous steps you can take to protect it better online. However, using social media, apps that track your location and websites that store cookies will not help your privacy. So it's clear privacy isn't a fundamental right on the Internet, but that doesn't mean you must go off-grid.

Find your measure of using advanced services and increasing privacy simultaneously. You can balance it with a proxy server as a great starting position, taking your time to study privacy settings and turning off location services as a follow-up task. A proxy checker can help you choose a proxy server, but there are no workaround privacy settings. If it bothers you, you must manually reject cookies on websites and play with the app and social media settings to eliminate as much tracking as possible.