A Student's Guide to Digital Privacy

[For Everyone!] [Find the most up-to-date version of this guide on UvicLinux.ca]

Introduction

I created this as a one-piece guide to a critical, but complex and constantly evolving issue. A reliable starting point to digital privacy, security, anonymity and freedom.

This guide is focused on the British Columbia context but is broadly applicable worldwide. After reading this guide, you'll understand why your data is important, and be equipped with doable steps to protect it. In **#Resources** and alongside the content, you'll also find videos, online communities, software, and other helpful information.

Change is a winding path, but you never have to walk it alone.

Contents

1. #Why Privacy Matters
2. #Privacy in BC and Canada
3. #Privacy and Activism in Canada
4. #Threat Modeling
4. #The problem with Big Tech
3. #Recommended Actions
4. #Best Practices
5. #Software Alternatives
6. #Resources+Credits

Note: Internal links are marked with a #.

Why Privacy Matters

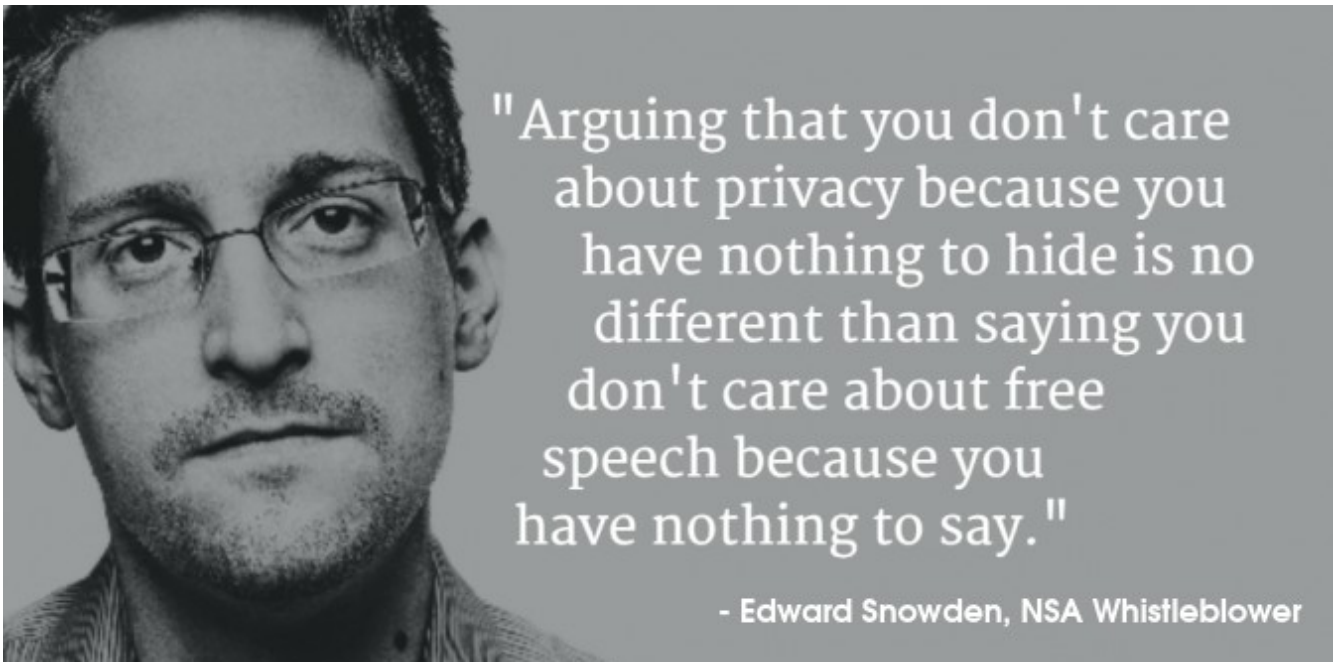
Privacy is a human right. It's why you whisper, use DMs, and close the bathroom door.

In short, privacy is an essential component of social justice. Surveillance capitalism goes beyond corporate interests, providing information to governments. Many movements that seek to improve the world are criminalised, particularly as fascist politicians get elected and seek to further repress dissent. A prime example is the Kids Online Safety Act (KOSA) in the USA, which would encourage sensitive topics to be pre-emptively censored, restricting access to everything from lifesaving mental health resources to basic social justice topics such as education about racial discrimination. One of its creators says it should be used to censor trans speech.

Geopolitically, on an even more extreme note, the CCP has access to data from Tencent, which has bought majority shares in Snapchat, Discord, Reddit, and other platforms. This has led to theories that the CCP knew about the events of January 6th at the US Capitol ahead of time, and is able to leverage world events to come out on top.

Privacy is both an end goal by itself, and a tool by which to allow change in the face of repression. It cannot protect individuals forever, but it can create space to work within.

Digital Privacy is a lot like the Climate Crisis. They both require widespread public awareness, political action, grassroots organizing, and lifestyle changes. Both issues are used misleadingly by corporations for marketing. And the best way to make progress in both is to **start with your friends and family.**



Privacy in BC and Canada

Canada has an Office of the Privacy Commissioner and a series of privacy laws. British Columbia has its own privacy laws relating to this, the main acts being PIPA and FIPPA. All of these set out guidelines and regulations around how organizations must handle and protect personal information, including requirements for obtaining consent, limiting the use of personal information to specified purposes, and implementing security measures to prevent unauthorized access or disclosure.

However, these laws are fairly limited and haven't kept pace with the modern internet. They are not functioning to protect people from corporations that require unreasonable amounts of information in order to use their service. They also are not used to protect people from mass surveillance, which is a growing concern and has been proven time and time again to be an ineffective method of policing.

Privacy and Activism in Canada

In Canada, you have the right to protest, provided that no laws are broken in the process. However, there are many ways a protest can be deemed illegal, and in this situation, your privacy matters. If you participated in a protest that was deemed an unlawful assembly, you can be arrested on scene or later on if your presence was identified. Wearing a mask at protests is a good way to protect your privacy, but it could lead to a strict sentence. It is now illegal to wear a mask at an unlawful assembly.

In Canada, police have the right to search your phone without a warrant. Thus, when attending a protest, you should keep your phone in **'lockdown'** mode, making it impossible for a police officer to unlock your phone with your finger or by pointing it at your face. They should not ask for your password as part of this warrantless search.

For more information about protesting, consult the BCCLA or EFF's resources.

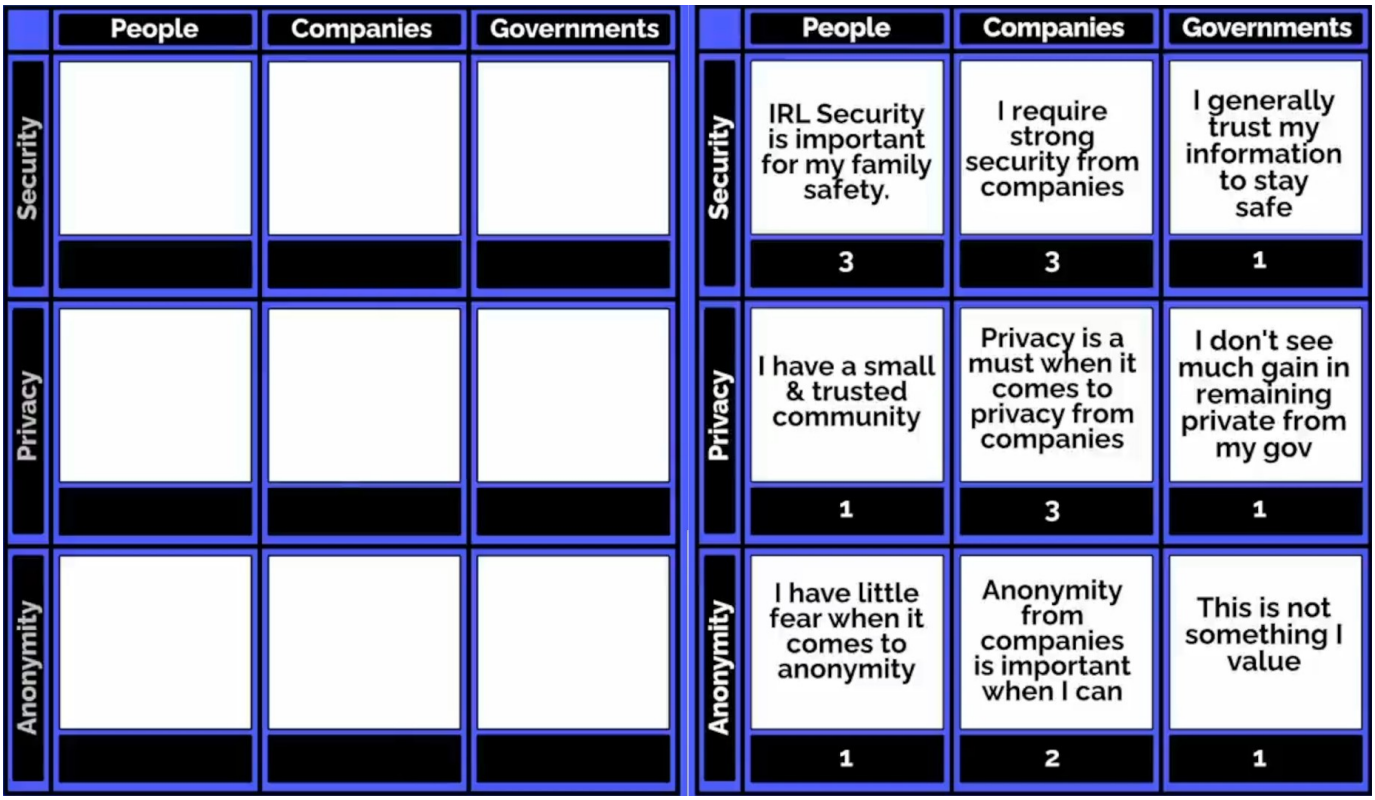
BC CLA BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

EFF ELECTRONIC FRONTIER FOUNDATION

Threat Modeling

Protecting your privacy online may require a lot of changes and planning. Every person and resource, myself included, will recommend different things. Threat modeling is just a fancy term for **"decide what you want so it's easier to achieve."**

- **Security** is the ability to protect yourself and your data from malice and accidents.
- **Privacy** is the ability to control who sees what parts of your activities.
- **Anonymity** is the ability to hide your identity (not necessarily hide your activities)



	People	Companies	Governments
Security			
Privacy			
Anonymity			

	People	Companies	Governments
Security	IRL Security is important for my family safety.	I require strong security from companies	I generally trust my information to stay safe
	3	3	1
Privacy	I have a small & trusted community	Privacy is a must when it comes to privacy from companies	I don't see much gain in remaining private from my gov
	1	3	1
Anonymity	I have little fear when it comes to anonymity	Anonymity from companies is important when I can	This is not something I value
	1	2	1

We all want different levels of Security, Privacy and Anonymity from People, Companies and Governments. This chart is one way to visualize that. On the right, 'Kevin' has explained and ranked the importance of each category. My personal chart is different, and yours might be too. See **Techlore's full video** on threat modeling for more.

The problem with Big Tech

Obtaining privacy from Companies is the most agreeable and widely discussed course of action in the privacy community. Thus there is no shortage of resources out there on how to do so.

This generally focuses on Big Tech, in particular, **Google Amazon Meta Microsoft and Apple (GAMMA)**. Each of these tech giants is in a dominant position in their respective sectors of the world. For Amazon, this is 'ecommerce' and server hosting, Microsoft, desktop computers and enterprise software, Meta, social media, Apple, the mobile market in North America. Google is particularly omnipresent - they dominate web search, web browsing, website analytics, advertising, video hosting, mobile phones, navigation, and much more.

There are many problems with the collection of this much data about individual people. For one, it can be seized by authorities, or caught up in a data breach if the company's security practices are poor. This is common with Facebook, for example. In addition, It takes resources to collect, transmit, analyse, store and use data, be it for advertising, algorithmic or other purposes. For many of their server farms, Google consumes cities worth of water supply to cool them.

Because of trackers, advertising, and other 'bloated' proprietary technology, the internet is far slower and more power hungry than it needs to be. **Privacy is sustainability.**

Lastly, as a moral and political principle, I believe **no one body should ever hold such power over the internet**, which connects and shapes the global human experience.

Recommended Actions

The following actions are highly recommended because they are **easy yet important**. These improve your internet experience, contribute to your general privacy, or achieve the most important steps in moving yourself away from Big Tech. They also teach people safer social media use and about the existence of alternative software, creating foundational skills that will last a lifetime.

If, like most people, you use Chrome and Google Search, near everything you do within these apps is known by Google. There are multiple good #open-source browsers for mobile and desktop that offer better privacy protections and general experience. My top recommendation is **Firefox.** You can also easily switch to a search engine like Brave Search, DuckDuckGo or Startpage. See #Browsing and #Search for more.

First of all - ***what is encryption?***

Encrypted data can only be decoded and understood by those with the keys. When people talk about encryption on the internet, they usually mean end-to-end encryption of information in transit. Did you know every website you visit that starts with `https://` is encrypted? Before this was standard, you could snoop on a public WiFi network and view all the emails and other info people were sending over the air.

If you use iMessage*****, WhatsApp, or Facebook Messenger your messages are already end-to-end encrypted. This means only you and the intended recipient can see the *contents* of your messages. The European Court of Human Rights recently declared encryption part of the human right to privacy. Despite this, at any given time, a government somewhere is considering a policy to surveil private communications, that would mean banning end-to-end encrypted messaging.

*****_iCloud backups are unencrypted, and so are conversations with non iMessage users. If you back up your messages with iCloud, the encryption is irrelevant. See #iOS for details._

Signal is a messenger designed with privacy from the ground up. The only data they have is the date a user created their account, and the date they last connected to the service. When US authorities subpoenaed Signal for data, this is all they got. This is virtually nothing in comparison to what Meta can collect about you through their messengers, even if the contents of your messages are encrypted. Because of this strong data policy, you don't have to rely on Signal or its employees for trust.

You (unfortunately) need to use a mobile number or landline to sign up for Signal. This makes it easy to find your contacts on Signal, because if they sign up (using the same phone number you have them as in your contacts), you'll get a notification. Keep this in mind if there's someone at home you need to hide it from. It has loads of features including large file uploads, video calls, voice calls, themes, photo editing, and stories.

Encourage your friends and family to contact you on Signal.

EFF's quick start guide for Signal

The more information you release, the more you have to secure and keep track of. No matter how ethical the platform you use is, you will be publicly sharing information about yourself. This can be dangerous. For example, remember that anything public on Instagram can be seen without an account or the app. In order of importance:

1. Remove all publicly available information you can. Use private accounts, and prefer spaces that aren't open to the entire internet.
2. Remove your legal name and face wherever possible. Most site's servers will keep deleted content, so governments could access it, but this protects your identity from bots, data brokers, employers, insurance companies, and the general public.

3. Instead of the app, use the websites for social media, and on mobile, use "add to homescreen." These are called **webapps**. The apps for social media sites collect more information about your device than the website can through your browser.

In #Socials you'll find ways to view certain sites anonymously and advice on how to delete your account(s). For more information visit EFF's guide to protecting yourself on social media.

Hundreds, sometimes thousands of individual domains connect to your device through websites and apps, gathering whatever they can. #Blockers are not a silver bullet, but they can speed up loading, save battery and eliminate ads, even on sites like Spotify. Apps like Safing Portmaster and Blokada offer granular control over what comes in and out of your device, but can also be "set it and forget it."

In addition to personal communications, your email may contain events, political views, login information, brand interests, and even banking information in addition to. This general-purpose service should be encrypted. It also acts as an identifier where you share it.

Create a **Tuta** or **Proton** account for free and move important communications to there. You can use a service like SimpleLogin to create aliases for logins, newsletters and other purposes without revealing your real email address.

Many of us have thousands of unread emails. This is a golden opportunity to change that. Accounts and subscriptions you don't want can be left behind, and with a clean slate, your new inbox can be kept minimal and tidy. See #Mail for more.

Best Practices

These are mostly attitudes and habits that are useful to have, and contribute to a healthier relationship with technology on a broader level, as well as promoting understanding and awareness around how things work and treat your data.

Digital Minimalism

You can Marie Kondo your digital world as well - and chances are, there's a lot of crap that does not spark joy, but it's easy to address. The more apps you have installed, the slower your device is and the more privacy and security vulnerabilities exist. One simple trick that has reduced the number of windows I have open is using Discord and Spotify in the browser. Remove things you don't use or plan on using - this includes bookmarks, email subscriptions, files, accounts and more. Organizing is a great lifelong habit.

Password Managers

This has multiple benefits regardless of your threat model. Your browser and brain's password storage is often insecure or unreliable. Good passwords are critical. Unlock your password manager with a strong passphrase and quit worrying about individual passwords for individual services - they can all have a unique, strong password, and you only have to remember the one passphrase. Use a trusted, open-source password manager like **Bitwarden** or KeePassXC for zero cost on all your devices.

Turn that off!

Next time you're bored, or setting something up, go through the settings of every device, app, and service you use. You can 'opt out' of data collection when possible, tailor settings to your needs, and better understand your software. Turn off radios when you aren't using them. On iOS, only the toggles *in the settings app* do this. On Android, go to settings > location and disable WiFi/Bluetooth scanning - now "off" means off. This saves battery and limits the effectiveness of location services, which may or may not be a positive for you. You can also disable your cellular radio with airplane mode.

Healthy Skepticism

If it was made recently and has an internet connection, it's likely tracking you. Smart watches, voice assistants, TVs, security cameras, cars, etc. Avoid purchasing these products wherever possible, and consult Mozilla's Privacy Not Included for reviews on such devices and ways to mitigate any privacy concerns that might exist within things you already own.

Support each other!

#Free and Open Source Software is built primarily by people volunteering their time for a cause or piece of software they care about. With the smallest of teams, open-source projects have created software that outperforms proprietary alternatives. This work is freely available - but depends on donations. With our funding, more people can work full-time to make FOSS alternatives shine.

And speaking of support, support your friends and family through the process of finding alternatives. You can do this out of passion for the cause or out of compassion for them.

About FOSS:

Source code is what makes software what it is. Open Source software makes this source visible, but also available for anyone to modify, fork (create your own version), and

contribute to. When the term "Libre" or Free is used, it means free as in freedom, not as in free beer.

Free and Open Source Software (FOSS) is often high quality and generally far more likely to respect your privacy. I almost exclusively recommend open source software.

Software Alternatives

Browsing

Brave

+ Better privacy than Firefox by default

- Contains some 'privacy-respecting advertisements', which can be turned off

- Chromium based

Syncing: Yes

Recommended settings:

- Set Trackers & ads blocking to Aggressive

Firefox

+ Highly customizable interface, extensible

+ Not based on Chromium web engine (support competing standards)

- Not fully privacy friendly by default

Syncing: Yes

Recommended settings:

- Change search engine
- Install Ublock origin
- Set Enhanced Tracking Protection to Strict

Consult this video if you wish to further 'harden' Firefox.

Switching to Firefox (Quick Guide)

Librewolf

+ Clean fork of Firefox (no Mozilla accounts, telemetry, etc)

+ Privacy-respecting and 'hardened' by default

- Desktop only, no built-in sync

Syncing: Best with external #sync software, or as a secondary/disposable browser.

Tor Browser

+ Access the Tor network, a series of decentralised relays that hides your IP address and gives everyone the same fingerprint.

+ Clear on exit – no cookies or history

- Slower connection, thus not good for use with accounts or streaming

Syncing: Best with external #sync software, or as a secondary/disposable browser.

DuckDuckGo Privacy Browser

+ A quick and easy way to switch away from Chrome and Google Search

+ Ad and tracker blocking by default

- Chromium based

Syncing: Best with external #sync software, or as a secondary/disposable browser.

Browser Isolation

Probabilistic tracking implies who you are based on device and browser fingerprints, IP addresses, etc. *Deterministic tracking* is based on your login, making it 100% accurate. While cookie isolation (a feature in Firefox) and blocking domains (with the Ublock Origin extension or Brave browser's shields) is good at keeping sites from seeing other activity in that browser, Browser Isolation is far more robust.

I recommend using a separate browser for every Big Tech site you log into. This also applies to accounts connected to them, e.g. "Sign in with Google". For example, I access one Google account in Chromium, another Google account within Brave, and Facebook in private Brave tabs, while Firefox is my main browser for everything else.

Note that your IP address is still an identifier - to obscure that, consider a VPN.

For more information on what VPNs can and can't do, see this article.

'Secondary/disposable browsers' clear cookies and history on exit. Using private tabs or separate browsers for different types of activities is always beneficial.

But what about syncing? You don't want to open something in the wrong browser because it's already in your history or bookmarks. The best solution is to store bookmarks in **XBrowserSync**, a FOSS, cross-platform tool for organizing them. Again, I recommend Bitwarden for managing your logins and passwords.

Comms

All of these feature end-to-end encryption.

Matrix

+ Decentralized, fully featured messaging protocol

+ Free instance provided by element.io

- User interface can be more complex, channels are not encrypted by default.

Session

+ Signal alternative that doesn't require personal information for signup

+ Near anonymity, impossible to shut down

- Far smaller userbase than Signal

Signal

+ Fully featured messenger with calls, video, themes, large uploads, stories, etc

+ Widely used, easy to discover contacts

- Requires phone number for sign up

Mail

Both recommended providers offer end-to-end encryption, calendar and contacts (an important compliment to email), and clients for Android, iOS, and web.

Proton Mail

+ 500MB free storage

+ More featureful interface

+ Paid users get access to a suite of privacy tools including Drive, VPN and more. Integrates with Simplelogin

Tuta

+ 1GB free storage

+ Clean, intuitive interface

Self-hosting

Running your own email server, locally or with a VPS (virtual private server) puts you in control of your email. For email alone, the above providers are convenient and secure enough to trust. However, owning a domain lets you host a variety of services. LandChad.net has guides on this.

Search

The following engines do not manipulate results based on personal data, and are funded by ads relevant to the search (which you can block of course). Their results are comparable to Google, or sometimes better, depending on the subject. For more advanced research, it's good to have multiple engines available. Many browsers have shortcuts to switch providers in the address bar when you're typing a search.

Brave Search

Uses its own independent search indexer, along with results from other engines when necessary. Continues to improve in terms of results.

DuckDuckGo

Draws results from Bing. Popular, trusted option, but some dislike the results.

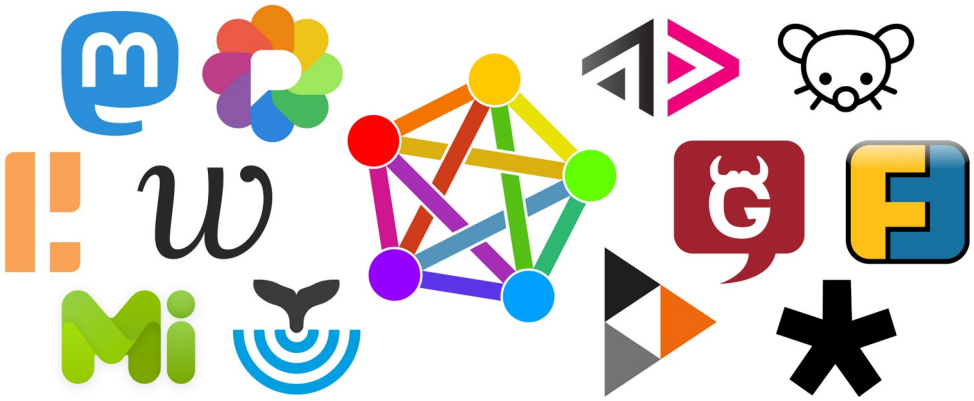
Startpage

Draws results from Google, results will look familiar.

Socials

The Fediverse

Since Elon Musk's purchase of Twitter, the Fediverse has been rapidly growing in popularity. It is a decentralised network of social media networks. It would be insane if you needed a Yahoo Mail account to communicate with your Grandma because she uses Yahoo, right? Yet this is how most social media functions. The Fediverse solves this quite elegantly. Mastodon, similar in concept to Twitter, is the most popular platform on the Fediverse, but there is also Lemmy, like Reddit, and PeerTube, like YouTube, along with many others.



Delete them

Whether you wish to leave one platform or multiple, here's how to do it smoothly:

1. Tell everyone! Create a post explaining why and when you're leaving. Provide ways for people to reach you or keep it to a per-DM basis - whatever you're comfortable with.

2. Be proud. Don't let people see it as a "goodbye" or "break." This is a ***move***.

3. Request your data, then delete your account permanently! This is why you're leaving :)

Frontends:

These allow you to view a site without logging into or creating an account. It's generally a game of cat and mouse to run these frontends, so at times, instances will be restricted or unavailable, but it's easy enough to switch instances. I use Invidious to view YouTube most of the time and it has been a positive experience.

Invidious (Youtube)

Libreddit (Reddit)

Nitter (Twitter)

Blockers

Blokada

A system-wide network manager for Android and iOS.

+ Encrypt DNS (take out of Google's hands)

- Cannot be used alongside a VPN on Android, though theirs is available for ~$6/month

Android install:

- Download and run the .apk, allow apps to be installed from 'unknown sources' if prompted
- After opening, add Blokada 5 as a VPN. Set as an "always-on VPN" so it doesn't disconnect.

iOS install:

- Install from the app store
- After opening, allow it to use your device's VPN slot

Completing setup:

- Tap Advanced > Blocklists and add at least one list. QISD does the job.
- Tap Advanced > Networks > Any Wifi/Mobile network, ensure DNS is encrypted and using an alternative provider such as Cloudflare (1.1.1.1) or Quad9 (9.9.9.9).

Safing Portmaster

A system-wide network manager for Windows and Linux.

+ Tracker lists already loaded by default

Windows setup:

- Download and run installer, that's it!

Linux setup:

- See if it’s in your distro’s repos. If not, you’re a Linux user, RTFM. At the time of writing Portmaster is not available on Flathub.

UBlock Origin

The best browser extension for blocking ads and trackers – works well on Firefox. Official Chrome neuters adblockers' ability to function effectively. Not necessary for Librewolf, DuckDuckGo Browser, or Brave, which have blockers built-in.

Desktop setup:

- Go to your browser's extension / 'addon' store and find it. Click the down arrows in the UBlock extension's popup view to see a list of the trackers each site loads.

Mobile setup:

- If you use Firefox on Android, you can install the UBlock Origin addon. At the moment, this is the only mobile browser that supports extensions.

Fix Your OS

Your **Operating System** itself is likely a big privacy offender. Android, iOS, Windows, and MacOS log user activity for advertising purposes, often on a level that's difficult to control. In this segment I offer solutions to this - some easy, some advanced.

Your device should be a tool for your needs, not someone else's surveillance device!

iOS and MacOS

Apple products are notoriously difficult to modify and have deeply embedded telemetry that cannot be disabled. However, an iPhone is arguably easier to deGoogle than a stock Android phone, so you still have lots of room to improve.

- Avoid iCloud - most major privacy concerns stem from this.
- Techlore's iOS guide: Invidious | YouTube
- Techlore's MacOS guide: Invidious | YouTube
- Your Apple ID is an advertising ID: Invidious | YouTube

Android

By default, Google knows every app you open, where you go and what you search, even when you thought things were disabled. Android is open-source though, and privacy-friendly projects exist. There are generally 3 ways to improve your privacy on Android, one for everyone.

Semi De-googled. Any Android phone can be used without a Google account - simply use privacy respecting services and apps from F-Droid, Aurora store to download apps from the Play Store, and use a tracker #blocker to control your apps' connections. Use Universal Android Debloater to remove all Google apps except Play Services, a privacy vulnerability needed in order to receive notifications. On a custom ROM, you can fully de-google and replace this with MicroG.

Custom ROMs. If you are open to buying, or already have a Google Pixel or other compatible phone, **CalyxOS** is easy to install and provides an up-to-date experience.

If you have another phone and technical expertise or the willingness to learn, this Advanced Android Degoogling guide will walk you through the process.

Buy a phone. If you lack the technical expertise to heavily modify your phone, but prefer Android and cannot stomach using a "Googled" device, these stores (among others) offer devices with privacy-friendly ROMs preinstalled. Each uses MicroG.

- Murena phones with /e/OS
- Rob Braxman's store
- iodé, EU-based seller

Windows

There's a good chance you're reading this on a Windows computer. It's a powerful, well-supported OS, but with a lot of telemetry baked-in, preinstalled applications, and disruptive updates. Luckily, PCs are inherently more privacy friendly than mobile phones. Here's how to improve privacy without ditching Windows:

- Avoid cloud services like Onedrive

- Use Windows defender, other antivirus software is generally counterproductive
- It’s better to use Microsoft Edge and tweak some of the settings than to install Chrome, though I of course recommend other open-source browsers.
- Run Chris Titus's toolbox; hit 'Essential Tweaks' to debloat your OS and disable telemetry in one click. You can also remove Cortana, Onedrive, enable dark mode, and more.
- Techlore's Windows guide: Invidious | YouTube

Linux

Linux is a kernel that powers spacecraft, supercomputers, and servers. But it’s also a term for the Linux desktop, a FOSS OS you can install right on your Windows PC. If you want an entirely FOSS desktop experience that gives you complete freedom, Linux is perfect for you. If you depend on specific proprietary software (such as the Adobe suite, Solidworks, ArcGIS) or your favourite game isn’t supported, you may want to dual-boot or stick to Windows for now. Linux gaming is very easy today thanks to Steam’s Proton.

To pick a Linux distribution or "distro", focus on community support and the package manager. Fedora is stable yet up-to-date with an intuitive desktop environment by default. Zorin and Pop!OS are also beginner-friendly distros with preinstalled Nvidia drivers if you have an Nvidia GPU. Note that their base, Ubuntu, is slow to update.

The best way to try Linux is to set aside a partition on your main machine's drive, a secondary machine, or a separate drive, and test every piece of software (including new alternatives) you want to use on your PC. Repeat until you've found what works for you and can commit to using it full-time. The switch will be easy if the software you use on Windows is already cross-platform, so you can transition that at any time.

Resources + Credits

Thank you

for reading this guide. You're one of the many people helping to leave the world better than you found it. If you think any part of this guide could be improved, have any feedback or comments, or would like any assistance, feel free to contact me.

This guide and the broader privacy community is possible thanks in part to the following content creators, websites and individuals. Please visit some of these links in your free time :)

Content:

- Techlore (High quality, active, respectable privacy channel)
  - Website | PeerTube | Invidious | YouTube
- Surveillance Report podcast (Current news, keeps me passionate, why it matters)
- Mental Outlaw (Humorous, covers popular events and opsec)
  - Odysee | PeerTube (Unofficial) | Invidious | YouTube
- The Hated One (Focus on anonymity and other social issues)
  - PeerTube (Unofficial) | Invidious | YouTube | Reddit (for sidebar resources)
- Wikipedia: Mass Surveillance

Resources:

- TOSDR (Summarized terms of service)
- Electronic Frontier Foundation
- EFF's Surveillance Self-Defense
- Pluja's Awesome Privacy
- Privacy Guides
- The New Oil
- UVic Linux Club (Friendly community for Linux users, software engineers and privacy advocates, graciously hosting this guide on their website)