DE-GOOGLE YOUR LIFE

Google deceptively monitor's, tracks and records everything about you without your knowledge or consent. Every product they make is designed to extract as much information as possible about you, and they use this data to influence what you buy, how you think and who you vote for. And they've mastered the ability to do this without your knowledge. It's time to exorcise the Google demon from your life, so you can once again be free.

PRIVACY™
ACTION PLAN
with GLENN MEDER

CONTENTS

WHY SHOULD I WANT TO DE-GOOGLE MYSELF?

Ten years ago, Google's slogan was "Do no evil."

But now, Google is the devil itself.

Google is tracking, monitoring, and recording everything you do online, from your searches to the websites you visit, your health, where you go, what your political beliefs are, who you talk to, what you buy, and what you say in your emails. They do this without your knowledge and without your consent. (Remember when consent was a vital human right?)

Now they are convincing people to put cameras and microphones in their homes so they can record your conversations, watch you and know every little bit about your life.

They create powerful commercials. They have wonderful gadgets that make your life easier. But at what cost?

Google's business model is dependent upon their ability to capture as much information about you as possible, and then use this data to influence you. They are extremely good at influencing and manipulating you without your knowledge.

They do all of this while telling you that they are protecting your privacy, which is a lie. They use deception, stealth, and an unlimited budget to manipulate you. They don't care about being sued, because whatever amount they get sued for pales in comparison to the titanic profits they make by being deceptive.

Google's deceptiveness has been proven over and over again. On one hand, it's amazing that people still trust them. But in reality, it's not a surprise because Google is one of the main perpetrators of censorship and control. They censor whatever doesn't fit the narrative they want you to know. They "deplatform" (ban) users and label certain searches and content with highly political "fact checks".

If you want to delve into the dark underbelly of Google, here are some important articles:

Google is Manipulating Voters on a Massive Scale.

The Shocking Amount of Data Google Knows About You.

Google Employees are Eavesdropping, Even in Your Living Room.

How Google Controls What You See Online.

Google is Tracking Your WebMD Visits.

Google's Response to the Hidden Microphone in the Nest Thermostat.

Google Collects Android Users' Locations Even When Location Services Are Disabled.

Google Admits It Lets Hundreds Of Other Companies Access Your Gmail Inbox

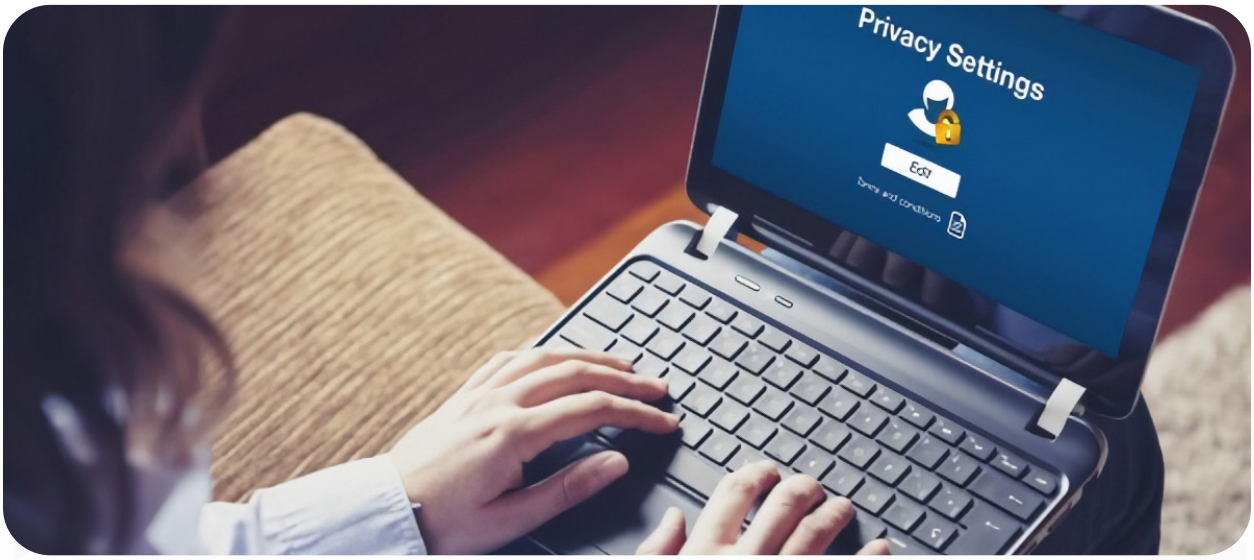
Google Faces Class Action For Allegedly Tracking Private Browsing Activity

Google Must Face $5B Lawsuit Over Tracking Private Internet Use, Judge Rules

You joined the Privacy Action Plan because you were worried about privacy. And rightfully so. The fact is, one of the most important things you can do to recover your privacy is to exorcize Google from your life. This document shows you how to do this. Welcome to your De-Google manual.

STEP 1

GETTING INFORMATION OUT OF GOOGLE



The first step is to remove your information from Google. Before you remove this data though, it's a good idea to download it and see what data they have about you. To see the data Google has about you, follow these steps:

1. Log into your google account.
2. To download all the data Google has on you, go to: https://takeout.google.com
3. Select **All**, scroll down and click on **Next Step**.
4. In section **Select the file type, frequency and destination**, select:
    - Delivery Method: **Send download link via email**
    - Frequency: **Export once**
    - File Type & size: **.zip** & **4 GB**

WARNING: If you have been using Google Services for years, the amount of data may be significant. Once you receive the download link, click on it and choose where you want to save the data. It will be in a ZIP file. Right click on the ZIP file and extract it, or if you are using a Mac, simply double-click it. This will create a folder that will contain additional folders.

STEP 2

REMOVE HISTORICAL SEARCH AND LOCATION DATA

Now we will remove all the information that Google has compiled from our searches and location data and prevent services from storing new information.

1. Log into your google account.
2. Go to Activity Controls and disable **Web & App Activity**, icon should look like this.

   - Disable both **Include Chrome history...** & **Include audio recordings** options. Click on "**Manage Activity**", this will take us to "**Web & App Activity**". Disable **Web & App Activity**. Scroll down to the "**Search your activity**" search bar, click on the "**Delete**" button, select "**All time**" in the new window, confirm you want to delete.

3. Back to Activity Controls, this time scroll to "**Location History**" and  it.

    - Still under Location History click on **Manage Activity.** Click on the **Year** at the top right corner of the screen and select **All**, if you cannot see All, just select any day from the list and then go back to select **Year** and select **All**. Click on the **trash bin** to delete All and confirm you want to delete all.

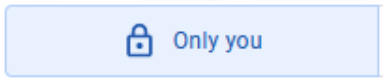
4. Back to Activity Controls, this time scroll to **YouTube History** and  it.

    - Disable both **Include the YouTube videos you watch** and **Include your searches on YouTube** options. Still under **YouTube History** click on **Manage Activity.** It should show **Not saving activity**. Scroll down to the "**Search your activity**" search bar, click on the "**Delete**" button, select "**All time**" in the new window, confirm you want to delete.

5. Back to Activity Controls, this time scroll to **Ad personalization.**

    - Click on **Go to Ad Settings**. Disable **Ad personalization**.

6. Now to Info you can share with others. You can also find it in the Data and privacy menu.

    - Click on **Profile**. Now click on **Gender** and click on the button. Go Back and click on **Birthday**, 

and set it to "Only you". Go back and scroll to **Contact Info**, leave Google Account Email, remove everything else. Scroll to **Work & Education** and remove everything.

STEP 3

DITCH THE GOOGLE CHROME BROWSER

With over 60% of the market, Chrome is the most popular browser in the world. Chrome is owned by Google, so it should not be used.

Chrome is the most intrusive browser on the market. It not only captures the data from Google-related services and tabs, but also from every tab that is open in your browser. It actively monitors, tracks, and records your information.

So, it's important to ditch Chrome. Before you ditch Chrome though, you have to get your alternative solution in place. There are browsers that respect your privacy, but it's important to not just rely on one browser. Consider having multiple browsers for different online activities. This is called **compartmentalization**, and it's a powerful strategy for remaining private.

For Example:

- Browser #1 will only be used for accessing your online accounts that require a password. You can stay logged in with only this browser, and it won't be used for general browsing.
- Browser #2 will only be used for web browsing, with various privacy configurations and no cookies or history being stored on the browser.
- Browser #3 could be completely locked down for maximum privacy and security.

Following this example here are a few browser recommendations and their specifications, get used to these Logos:

Mozilla Firefox
https://www.mozilla.org/en-US/firefox/

Brave Browser
https://brave.com/

Mozilla Firefox: Firefox is a great browser. It respects your privacy and has features such as "permanent private browsing mode".

Brave: Brave is a fairly new browser that is focused on user privacy. Brave has an adblocker that prevents annoying adds, blocks trackers and has background video/audio playback, which is a great feature to listen to videos/music while the phone's screen is off or if you are doing different tasks with the phone. It does not send any sort of information back to Brave on exit.

1. **Choose the browsers** you want to use. **Download** them and **install** them.
    a. For **Firefox**, go to https://www.mozilla.org/en-US/firefox/ for your computer, or go to your app store on your phone.
    b. For **Brave**, go to https://brave.com/ for your computer, or go to your app store on your phone.

2. **Export bookmarks** from Chrome (if necessary).
   a. Click on the three parallel lines in the top-right corner of the ⋮ window.
   b. A drop down menu will appear. Click **Bookmarks**. It will prompt a pop-out menu.
   c. Click **Bookmark** manager. It will open in a new tab.
   d. Click the 3-dotted icon located on the far-right side of the blue banner, and select ⋮ **Export bookmarks**. Type the name of your bookmarks file and select a location for the file, then click **Save**.

3. **Import bookmarks** in another browser (this works in any platform and for our browsers).
   a. Press COMMAND + SHIFT + O (in Mac) or CTRL + SHIFT + O (in Windows), the Bookmark manager will appear. Look for **Import bookmarks** or **Import and Backup... Import Bookmarks from HTML.** (The keyboard shortcuts should work in all browsers, if it doesn't, go to **Settings**... then to **Bookmarks**.)
   b. Locate the file you saved previously, select it and click **Open** or **Import.**

STEP 4

YOUR SEARCH ENGINE

In the previous step you changed your browser. The single most important thing you need to do to set your browser up properly is to switch your default search engine to Brave, Presearch, or SwissCows.

In the USA, 87.6% of all web searches happen on Google. If you use Google as your search engine, they record every search that you've ever made. They know where you go, what your interests are, and the skeletons in your closet. Yes, it's possible to go in and adjust your settings to have Google erase your data, but how do you know that Google actually erases it? Google has been caught lying so many times that it's clear that you simply shouldn't trust them.

But it goes far beyond deception. Google can control your perceptions about an issue by controlling the results you get and even the auto-fill options (but you will not be aware that you have been manipulated). Reports show that they can have a significant impact on election results.

WHAT TO DO...

One of the most important things you can do to protect your privacy is simply stop using Google as your search engine. I don't recommend Bing or Yahoo either, because those are big tech companies that also take your information.

Instead, I recommend that you use Brave, Presearch, or SwissCows. All three of these search engines are good and private. I personally use Brave and I love it. The search results are just as good as Google's.

To drop Google and use one of these other search engines, you have to change your default search engine, which is very simple to do.

TO CHANGE TO **BRAVE**...

To get instructions on how to change to Brave, simply go here.
This link will detect what browser you are using and will give you simple instructions on how to make this change in your particular browser (i.e. FireFox, Safari, Chrome, Edge, Brave, etc.)

TO CHANGE TO SWISSCOWS.COM...

If you would rather use SwissCows.com, go here.

To Change to **Presearch.org**...

If you would rather use a decentralized engine, use Presearch.org, go here, look at the pop-up window that will detect your browser, and just click on **Add Presearch to Firefox/Brave.**

DON'T FORGET...

Remember to do this in every browser you use on every device that you use, including your mobile and desktop browsers. Also, remember to remove any links or shortcuts that you have to Google, Bing or Yahoo.

STEP 5

GMAIL

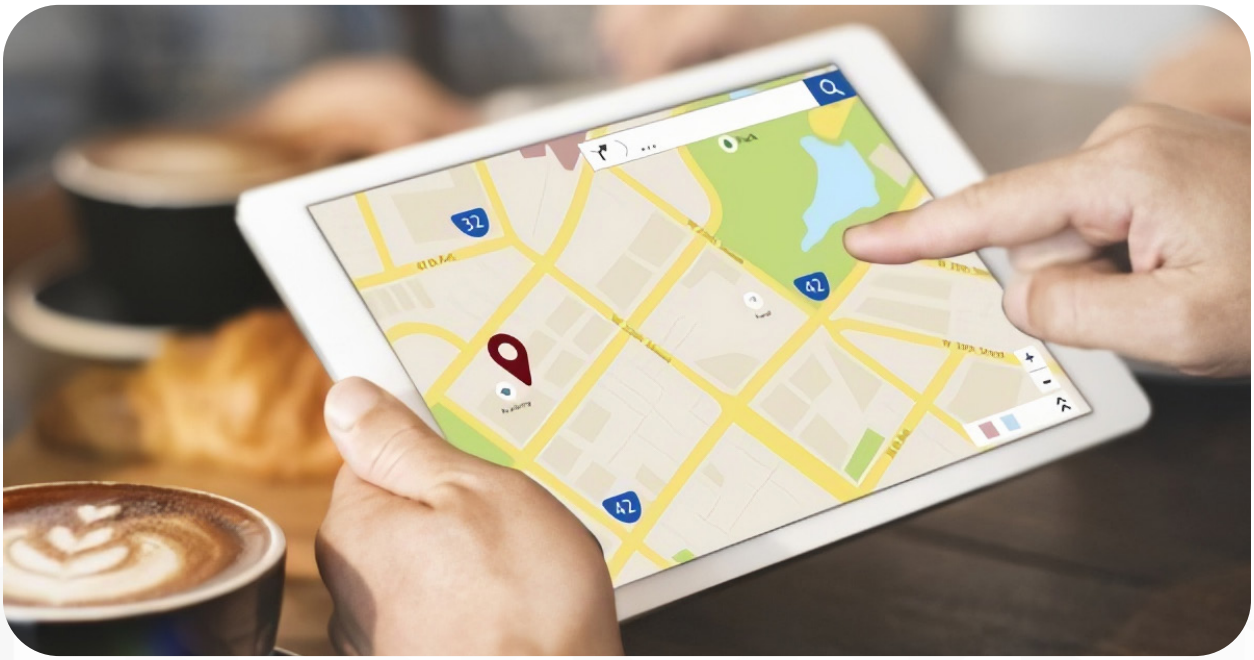
It is essential that you get away from Gmail. Not only does Google look at your emails, but they also let hundreds of other companies look through your emails. Google employees can look through your inbox too.

We recommend either ProtonMail or Tutanota.

We provide extensive training on this process in the Privacy Action Plan, and a brief explanation would leave out important steps. So refer to our Private Communications Chapter for more information on this step.

STEP 6

NAVIGATION GOOGLE MAPS AND WAZE



Some people rely on Google Maps every day. Unfortunately, Google Maps and Waze are both owned by Google, so they are capturing everything about you.

So here are some options for moving away from Google Maps. Try these apps and see which ones have the features that work for you...

OsmAnd

Here WeGo

Magic Earth

OpenStreetMap

To download them onto your phone or tablet, go to your app store or play store.

STEP 7

REMOVE YOUR HOME'S IMAGE FROM GOOGLE MAPS

While we are on the subject of maps, Google also has a service called "StreetView". With StreetView, you can type in any address and then click to see what the property looks like from the street. Not only is your home's image captured, but it could also include an image of your cars, and even you and your kids.

We cannot delete the data that the "Google Car" captured, but we can request that Google blur our house, car, driveway, or whatever other property that we do not want anyone to see.

SIDE NOTE: Did you know that the same car that was taking 360° pictures of your neighborhood was also recording the available WiFi networks? That's the way Google can still track you even if you have your location services off.

If your WiFi is always on, Google can see the available WiFi networks in the area you are in. As soon as it detects a known network, it will guess your location and send back the information about the new WiFi networks available. This means that we are constantly feeding the beast with more data for their location services. **ACTION:** Always turn your WiFi off and only turn it on when needed.

Steps to do this...

1. Go to maps.google.com
2. Run a **search** to find exactly what you want Google to Blur.
3. Drag and drop the **Street View Icon** to where you want to go. 
4. At the top left corner, beside the street, you should see the location icon and three dots. 
5. Click on the three dots and select **Report a Problem.**
6. A new window will show up where, by clicking on it, you can adjust the image to focus on the part we want to blur.
7. Under the photo, go to **Request blurring** and select the **appropriate object**, fill in a little **description** about it, enter your **email address**, complete the **reCAPTCHA** and submit.
8. Google will queue your request. You will receive an email confirming your request and a second email, this may take a few days, when the image has been blurred.

STEP 8

GOOGLE DOCS

Everything that you write and create with Google Docs will be analyzed and recorded by Google, so don't use Google Docs. There are good private alternatives. Do they offer everything that Google Docs offers? No, because Google has an endless budget to create great products designed to steal your data. These options are still very good, and they don't steal your data.

Apache OpenOffice – Alternative to Google Docs, it's a well-known open-source office suite platform that is also available offline.

Another option that is new is called www.Skiff.org. This service is in beta right now, so be ready for some hiccups while using it. Do not move everything you have before testing it first.

STEP 9

GOOGLE DRIVE

It goes without saying that you should move everything off of Google Drive. Here are some private and secure alternatives.

NextCloud

Sync.com

Tresorit

STEP 10

YOUTUBE

YouTube was acquired by Google in November 2006 for US $1.65 billion. Since then, it has started applying the same policies that apply to all its services, which is mass surveillance.

YouTube recently started censoring videos, channels, and creators, denying freedom of speech. Other people have been demonetized, which means that YouTube doesn't pay them for the advertising that appears on their videos (YouTube still makes money from the ads, but it doesn't share it with the content provider).

It's not enough to sign out of YouTube, because YouTube can still track you. Signing out of YouTube (and Google) is an absolute must, so this is our first step.

First, **sign out** of YouTube in your browser. To do this, simply go to youtube.com and make sure you are signed out by clicking on your username (photo) at the top right and select **Sign Out** in the drop menu.

ALTERNATE SOLUTIONS.

For Mac, Windows, and Linux, the best way to privately use YouTube is to use FreeTube. FreeTube is an open source, privacy-focused app that is designed to give you access to all YouTube videos while preventing YouTube from capturing any of your data. **NOTE: The website is https://freetubeapp.io (do not go to FreeTube.com because that is a porn site.)**

FreeTube is not a separate video platform like Rumble. Instead, FreeTube allows you to view all videos on YouTube via a proxy server, which hides your user data from YouTube. With FreeTube, you can watch videos, subscribe to different channels, save videos, and view trending videos.

While YouTube can still see your video requests, it can no longer track you using cookies or JavaScript. Your subscriptions and history are stored locally on your computer and never sent out. Using a VPN is highly recommended to hide your IP while using FreeTube.

d. The interface is very lightweight and allows you to download the videos by simply right clicking and selecting **Save Video As...** You can subscribe to channels, create playlists, and even IMPORT subscriptions from your YouTube user (not playlists though):

e. To import your subscriptions:

In a separate browser Open Google Takeout.

1. Under Create a new export choose YouTube and YouTube Music.
2. Click on "All YouTube data included" and only tick "subscriptions" in the dialog that opens.
3. Click on Next step, make sure Export once is chosen and click on Create export.
4. Wait until the export creation is finished, then on the same page click on Download under your latest export, which should now be visible.
5. Extract the downloaded archive and find the file subscriptions.json.
6. While logged into your Invidious account, go to Subscriptions -> Manage Subscriptions -> Import/Export -> Import YouTube subscriptions, select the file you just downloaded and click on Import.

For Android, there's an alternative to YouTube named **Vanced**. It works like YouTube but without tracking you. Remember to not sign in once you have installed it.

You can enjoy ad-free, background sound version of YouTube, to install **Vanced**:

a. Use your Android browser to navigate to https://vancedapp.com/

b. Tap in the blue button showing **Vanced Manager (vX.X.X)**

c. Follow the screen instructions to install **Vanced Manager** and the rest of the necessary files.

4. Our last option is to use other streaming platforms.

Due to the banning and censorship actions that began last year, plenty of other video streaming platforms have started to flourish. Freedom of speech is their primary business, but this doesn't mean they are privacy oriented, so use them at your own risk.

https://d.tube/ https://www.dailymotion.com/ https://www.crackle.com/

https://vimeo.com/ https://rumble.com/ https://www.bitchute.com/

[1]**A proxy server** provides a gateway between users and the internet. It is a **server**, referred to as an "intermediary" because it goes between end-users and the web pages they visit online.

STEP 11

GOOGLE CHAT

Used still by a few, Google Chat is a chatting programs.

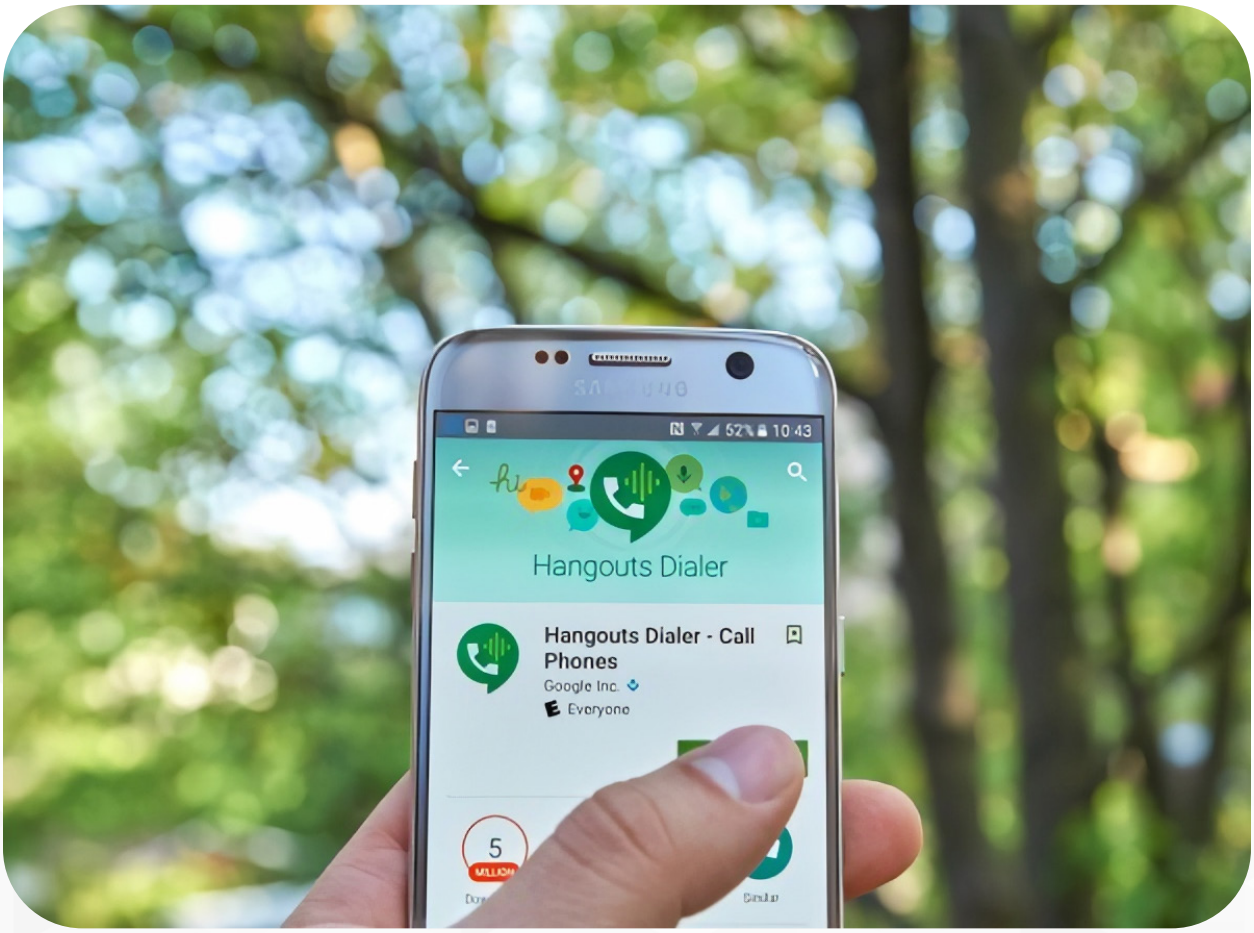
To replace Google Chat, we recommend Signal. Stay away from Facebook Messenger and WhatsApp.

Signal

https://signal.org

STEP 12

GOOGLE HANGOUTS



Google Hangouts is a conferencing platform.

There are two good replacements for Google Hangouts, depending on your needs.

If you are simply video conferencing with a few (up to 16) friends, Signal can work well. It is private and secure, and you can install it on your phone, tablet, or desktop.

For professional business meetings, we recommend a brand new service from Brave. Yes, the same Brave that has a browser and search engine. This new service is called Brave Talk, and can be found at https://brave.com/talk/ This of this service as a private, secure version of Zoom.

STEP 13

ANDROID, COMPLETE DE-GOOGLING

Android OS the one mobile OS to “slave” them all...

Android, developed by Google, is probably the most intrusive software that has ever existed. Of course, it is designed for your convenience, but there is a deeper, more sinister motive. By controlling your phone, they know everything about you, from where you go, who you talk to, what you do online, what you purchase, and much more.

The simplest solution is to upgrade to an iPhone. Apple has better privacy protections than Google because their business models are different. Apple makes its money by selling you products and services, while Google is an advertising company that makes money by gathering your knowledge.

But while Apple is definitely better than Google, we don’t trust Apple either.

So what are the other options? Not many at this time.

There are privacy phones in development, such as from e.foundation, but we haven't found one that we can yet recommend.

The other option is to actually install a de-Googled version of Android on your phone. We have a section on our course that teaches people how to De-Google their phones and install CalyxOS. Be assured that open-source, privacy-based software is quickly improving, so we expect to see easier ways to install a de-Googled operating system soon.

If you are willing to try it, the simplest de-Googled operating system is CalyxOS.

CalyxOS is a de-Googled Android mobile operating system that puts privacy and security into the hands of everyday users. Plus, proactive security recommendations and automatic updates take the guesswork out of keeping your personal data personal.

It has its own group of apps installed by default, like **Signal**, **Tor Browser**, **VPNs,** and there are special Market/Store Applications for you to download privacy-based alternatives to the most common apps you use, like F-Droid and Aurora Store.

As of today, **CalyxOS** can be installed on the following devices:

- Xiaomi Mi A2
- Pixel 2 and 2 XL
- Pixel 3 and 3 XL
- Pixel 3a and 3a XL
- Pixel 4 and 4 XL
- Pixel 4a and Pixel 4a (5G)
- Pixel 5 and 5a
- Pixel 6 and Pixel 6 Pro

STEP 14

ANDROID AND IOS, BLOCKING TRACKERS AND SYSTEM APPS

We saw in our previous step how to de-google ourselves by installing a different operating system on a Google Android phone, here's another option you could consider.

For this option, you need to follow two steps:

1. Setting up a **Private DNS server**[1]. To completely block online trackers, annoying ads, and protect your devices from malware sites and google tracking. This way even if you are not in a VPN, all your connections will go through a privacy friendly server that prevents all your traffic from being tracked.

2. Installing an APP on your phone that will work as a VPN with which you will be able to prevent traffic from any APP, including system APPS. Yes, including system APPS, all those Google and Apple apps that are "invisible".

3. Choose a DNS you want to use. We recommend: https://decloudus.com/ or https://www.cloudflare.com/dns/

Look for instructions on how to set it up on your phone depending on your operating system and/or version:

Decloudus. Scroll down the main site to the part where it shows **How to Connect Your Devices**, click on the device you want to configure and follow the steps.

Cloudflare, for iOS and for Android, for both, follow the instructions shown in section: Configure 1.1.1.1 manually.

With the above, you have secured your connection, neither ISP, or big Tech can see where your connections are going.

The next step is to block all **non-essential** applications from communicate. By non-essential, I mean anything that you don't recognize, should be blocked.

4. Depending on your phone, you need to install the correct APP:

Android – Download and install **NetGuard** from the Play Store.

iPhone – Download and install **Lockdown** from the App Store.

These applications are very similar. Once you open them, you will see a banner saying that the APP will establish a VPN connection. This is only because the APP will control what traffic goes in and out of your phone.

With **NetGuard** you can block the ability of APPS to connect to the internet either through WiFi, mobile network or both, by simply tapping the correspondent network icon. You can choose to show the system APPS by clicking in the icon with the three parallel lines that look like a funnel. (Warning: this may be overwhelming at first because there are hundreds of them; however, you cannot break the phone, so block them all except the ones you are familiar with.)

With **Lockdown**, has the ability to completely lock **trackers**[2] from any company, which will prevent them from communicating and sending trackers to their respective companies.

[1]**Private DNS Server** – The Domain Name System (DNS) maps the web address that you search (like privacyactionplan.com, otherwise called the URL or Unified Resource Locator) to a set of IP addresses so that packets are efficiently sent over the internet.

Generally, a DNS server will perform the translation from URL to IP. This process is called a DNS transaction, and these occur every time you visit a website, use particular applications, or communicate over specific platforms.

By default, these transactions, like the domain names, are unencrypted.

However, **Private DNS servers** encrypt the communication between your network and the DNS server and prevent third parties from intercepting the data by utilizing DoT and DoH technologies.

[2]**Trackers** – Trackers are files that originate not just from the Facebook and Google apps; they are embedded inside other apps you use every day, as well as the websites you visit with your mobile browsers.

This happens even if the app isn't active in the foreground and when you're not using your phone.

They silently collect data on what you're looking at, your actions–every swipe, tap, and button click–your location, and more. When this data is collected, it's sent out to advertisers, data brokers, and analytics companies.

By collecting this data on individuals from different sources, these companies build super-specific ‘shadow’ profiles of each individual.


PRIVACY™
ACTION PLAN
with GLENN MEDER