Android Privacy Guide

> Written by Attendz at https://gitlab.com/Attedz/AndroidPrivacyGuide

This is a list of **privacy-respecting** apps and services to replace ones that harm your privacy. All suggestions here do not require root access unless specified otherwise. *Please share your apps/thoughts and help to improve this list*! 👍

Apps/services must meet these requirements:

- Open-source because we cannot verify what closed source apps are really doing
- Does not collect user data or absolutely minimal that can't identify user
- Easy to setup

I, Attedz, am not affiliated with any apps or services.

Table of contents

- Password Managers
- Note-taking Apps
- YouTube Alternatives
- Ad blocking on Android
- Miscellaneous Apps

Operating System (OS)

You should not use the stock ROM that comes on your device. Stock ROMs includes **proprietary** (like Google Apps such as the Play Store and Google Play Services) apps and services that **spy on you**. Google even tracks your location when it's turned off.

Operating Systems listed below will not spy you.

LineageOS

> Operating system that respects your freedom.

RattleSnakeOS

> Privacy focused Android OS with advanced security features.

> NOTE: You need to build this by yourself.

microG

> Open-source alternative for Google Play Services.

> You can also check out LineageOS for microG.

> Note that **microG isn't operating system**.

Magisk

> Open-source and most popular root method.

> WARNING: **DO NOT** use SuperSU. **It's closed source and owned by Chinese company**

> Note that **Magisk isn't operating system**.

AsteroidOS

> Open-source operating system for smartwatches.

App Stores

Do not use Google Play Store. It collects information about your installed apps and Google even has ability to **remove and install apps without your permissions**.

App stores that are listed below are open-source and respect your freedom.

F-Droid

> Community-maintained software repository of FOSS (*Free and Open-Source Software*) apps.

> You can also add your own respositories.

YalpStore

> YalpStore allows you to download apps from Google Play Store without violating your privacy.

> You can also check AuroraStore which is fork of YalpStore with material design.

Browsers

Do not use Google Chrome. It's huge spyware and **will track everything you do online**.

Browsers that are listed below will not track you and are open-source.

Bromite

> Chromium based browser with built-in ad blocking and privacy enhancements.

Fennec F-Droid

> Firefox-based browser which removes the proprietary bits found in official Firefox.

Firefox Klar

> Surf and forget. Klar will delete all your data when you exit browser.

> WARNING: Firefox Klar version have WebRTC leak and it cannot be disabled.

Privacy Browser

> Privacy Browser protects your privacy by disabling features like JavaScript, DOM storage, and cookies that are used by websites to track users.

> WARNING: Privacy Browser is susceptible to MITM attacks when browsing insecure websites from devices running Android KitKat.

Search Engines

Do not use Google search. **It builds a profile from your searches** and knows your location.

Search Engines listed below do not build a profile about you.

StartPage

> Uses Google search to provide results. Google will only see StartPage, it will not see you.

DuckDuckGo

> DuckDuckGo doesn't save your searches or your location. Provides Yahoo and Bing results.

> WARNING: Based in the US and hosted on Amazon servers.

Searx

> Provides search results from multiple search engines, including Google search. Run by an individual.

> If you don't trust individual persons then use Searx by Disroot.

Messengers

Do not use closed source messengers like WhatsApp, Telegram, Hangouts or Threema. We can't verify what they are really doing in background.

Messengers that are listed below are open-source and are encrypted so no one can read your messages.

Wire

> Switzerland based company and doesn't collect information about users. Can also make calls.

[Conversations] (https://conversations.im) - [Free on F-Droid] (https://f-droid.org/en/packages/eu.siacs.conversations/)

> Client for Jabber/XMPP protocols. Can't make calls.

> You can host your own XMPP server or select from trusted providers. Good lists of providers are the Official list from Conversations or the Public XMPP servers list.

Some trusted providers:

> [XMPP.is] (https://xmpp.is/)

> Based in Germany and doesn't collect users messages or IP addresses.

Matrix - Download client on F-Droid

> Matrix is open-source decentralised protocol, it can do 1on1 and group chat with support for end to end encryption. Supports voice and video calls. There are gateways to chat across different networks.

> There are multiple clients. The official one is called Riot, which is provided as desktop app, mobile app and web client.

> WARNING: Official Matrix server collects a lot of metadata. Consider using another provider or host your own.

Briar

> Doesn't rely on a central server and works without Internet (through Bluetooth or Wi-FI). Also hides metadata. Can't make calls.

> WARNING: I'm not sure how reliable this messenger is and how many bugs it's have.

Signal

> Encrypted messenger & calling app. Doesn't collect information about users.

> WARNING: Signal is based in the US.

Silence

> Silence is a full replacement for the default text messaging app. Encrypts your communications between other Silence users.

> WARNING: For non-Silence users communications isn't encrypted.

QKSMS

> QKSMS is an replacement to the stock messaging app

> WARNING: Communications isn't encrypted.

Email Providers

Do not use Gmail. It's owned by Google which **scans all of your emails**.

Email providers that are listed below do not read your emails.

Tutanota

> Open-source encrypted email provider located in Germany. Also encrypts metadata. Free plan with 1GB storage.

> Also have paid plans.

> Tutanota offers beta app that works without Google Play Services. They are planning to publich app on F-Droid too.

Posteo

> Email provider that doesn't collect your personal information. Based on Germany. *1€/month*

> WARNING: Encryption isn't on by default.

ProtonMail

> Encrypted email provider based on Switzerland.

> WARNING: Doesn't encrypt metadata.

K-9 Mail

> K-9 Mail is an email client.

OpenKeychain

> OpenKeychain uses encryption to ensure that your messages can be read only by the people you send them to.

> Primarily integrates with K-9 Mail to provide end-to-end encryption capabilities.

VPN Providers

Getting good VPN is important on Android.

All VPN providers listed below have **"no logging" policy**.

> NOTE: You can never fully trust a VPN service. **There have been many cases where a VPN service claimed not to collect logs but still logged everything**.

> You are just **moving your trust from your ISP to the VPN provider**. If you need real anonymity use Tor or Tails.

Mullvad

> Based in Sweden. €5/month and supports Bitcoin.

ProtonVPN

> Based in Switzerland. 3 paid plans.

> There is also free plan but it's limited.

SigaVPN

> Based in the US. Doesn't cost anything, but you can get extra services for donating.

> WARNING: Service is based in the US.

> It's free, but the developer has said that it doesn't log anything and is run by donations and users that cryptomine for the service (optional).

> *Use with caution*!

OpenVPN - Download on F-Droid

> OpenVPN is client for connecting to your VPN Service through configuration files.

VPN Services to avoid:

These services are known to be harmful to your privacy and should never be used.

- IPVanish
- Hotspot Shield
- PureVPN
- Private Internet Access*

*PIA **is not known to be harmful** for your privacy, but **it does have some bad points to consider**:

- PIA recently hired *Mark Karpeles* as CTO.
- PIA is based in the US. Yes, *SigaVPN is based in the US too*, but **when you pay for the VPN service you need to get the best privacy possible** and with PIA **you won't get it**.

Cloud services

Do not use Google Drive for cloud storage solutions. It's owned by Google and **reads all your files**.

Google Photos is not recommeded either because Google scans all your photos and videos.

All cloud services listed below do not access your files. **Always encrypt your files before uploading them to cloud services**.

Nextcloud

> You can host your own Nextcloud or use one of the trusted providers below.

Cryptee

> Cryptee is a cross-platform, zero-knowledge, client-side AES256 encrypted, Documents and Photos service.

> You can sign up with just a username.

Syncthing

> Synchronizes your data between two devices. There is no central server that might get compromised.

Nextcloud Providers:

> [Woelkli] (https://woelkli.com/en) FREE/PRO.

> [Disroot] (https://disroot.org/en/services/nextcloud) 4GB/FREE.

File Sharing Apps

Transfer your files securely between devices.

TrebleShot

> TrebleShot allows you to send and receive files without an internet connection.

NitroShare - Download on F-Droid

> NitroShare is completely free of ads and trackers. Works on multiple platforms.

KDE Connect

> Integrates your Android phone with KDE desktop environment.

Password Managers

Creating strong passwords is an important part of privacy & security so that your accounts are more difficult to compromise.

Edward Snowden on passwords.

All password managers listed below are open-source.

KeePass DX

> Fork of popular KeePass for Android. Offline only.

Bitwarden

> Bitwarden can sync your passwords across all of your devices.

Passit

> Passit is an open-source, cloud-based password manager.

Password Store

> Can be synced with your cloud provider.

> Uses GPG key to encrypt data.

Note-taking apps

You shouldn't use Google Keep because Google reads all your notes.

Note-taking apps that are listed below do not read your notes.

[Standard notes] (https://standardnotes.org/)

> Encrypted note-taking app that can sync your notes across all of your devices.

Joplin

> Open-source and encrypted note-taking and to-do application. Can sync between devices.

> Good replacement for Evernote.

[Simple Notes] (https://github.com/SimpleMobileTools/Simple-Notes)

> Local note-taking app. Doesn't have encryption.

YouTube Alternatives

Watch YouTube videos without harming your privacy.

App: NewPipe

> Watch YouTube on your smartphone without annoying ads and questionable permissions.

App: SkyTube

> SkyTube is an alternative, free, open-source YouTube application for Android.

Website: Invidio

> Invidio is an alternative to HookTube.

Website: CloudTube

> When watching a video, no contact is made with the YouTube API.

Ad Blocking on Android

Blokada

> Open-source ad blocker. Use AdAway if you have *rooted device*.

> User can also change DNS address on Blokada.

NetGuard

> Block apps from accessing Internet. Use AFWall+ if you have *rooted device*.

> User can also change DNS addresses on both apps.

XPrivacyLua

> Feeds apps with fake data instead of your real personal data.

> *XPrivacyLua is not ad blocking app but it will reduse risk of your personal data to leak*.

> **Root and Xposed required**.

Privacy respecting DNS servers:

> UncensoredDNS

> Based in Denmark and doesn't log users (*only logs traffic volume*).

> SecureDNS

> Based in Netherlands and doesn't log users.

DO NOT use Cloudfare's DNS servers. Cloudfare is not privacy respecting company.

Miscellaneous Apps

Gboard

> AnySoftKeyboard doesn't collect information about users.

> Simple Keyborad for users that don't need extra features.

> Hacker's Keyboard with advanced features.

> AOSP keyboard that comes pre-installed with many Custom ROMs.

Simple Mobile Tools

> A group of simple and open-source Android apps without annoying ads and unnecessary permissions.

Open Camera

> Completely free, and no ads.

OsmAnd

> Maps & Navigation app that respects your privacy.

andOTP

> Use this app to control your two-factor authentication codes.

> Fork of OTP Authenticator.

EDS Lite

> EDS allows you to store your files in an encrypted container.

LibreTorrent

> Torrent client for Android with advanced features.

mpv

> Video player based on libmpv.

Slide for Reddit

> Open-source, ad free Reddit browser.

Pedometer

> Pedometer app to count your steps.

Voice

> Audiobook player.

AntennaPod

> Podcast manager and player that gives you instant access to millions of free and paid podcasts.

DO NOT USE FACEBOOK

Facebook is known for **listening to your microphone without your permission** (there isn't any **official** proof, only many reports) and gathering all of your data.

> Two well explained Reddit posts about Facebook listening: Post 1 and Post 2.

Retrieved on 20 Dec 2019 from https://gitlab.com/Attedz/AndroidPrivacyGuide for goodopsec.org