GET PRIVACY FREEDOM Privacy Phone

[Getting Started & User Guide]

For more SETUP and OS info visit our Resource Page at https://getprivacyfreedom.me/get-sovereignty/, and visit https://e.foundation/.

System Updates: Your OS (operating system) will notify you when there is update available. Download & install the latest update. When you reboot, you will notice a completely different screen loading / bootloader unlocked, etc. This is normal.

Activation: In most cases, you can simply transfer your SIM card into your new Privacy Phone & reboot. You may need to get a "Sim Card Kit" and work with Service Provider if having any data connection issues. Remember to TURN ON Mobile Network toggle!

Transferring Data: For Android to Android you can easily transfer Messages, Call logs, and Contacts, using ***Smart Transfer: File Sharing*** App by Aomata, found on Play Store / App Lounge or the ***SMS Import / Export*** APP on Droid-ify or Fdroid store. Iphone to Android is a bit more complicated and details can be found in our FAQ's *https://getprivacyfreedom.me/faqs/*. Can transfer photos by saving them to a USB-C drive or uploading to a Cloud like mega.io.

App stores:

- *App Lounge* – This is your main APP STORE and has about anything that Google / Apple store has. CAUTION: There is currently no App on this phone that is connected to YOU. There is No Google / Apple ID needed for this store. SO, be careful what is downloaded. One "bad" APP can expose you.
  - *Closed Source vs Open Source* - It's best practice to use *Open Source Software* which means the code is *open* for all to see what's inside of it (spyware, etc). You can check this when you click on an APP. There is a Privacy Rating & Privacy Analyses provided that shows *Permissions* needed and *Trackers*. Big-Tech APPS like Tik-Tok require Permissions to all of your sensors and have Trackers. This is dangerous if want to maintain anonymity on your device.
  - *Open Source APPS* –If only want to see Open Source APPS, then go to *Settings → Show applications*, and click on *Show only open-source apps*. Use discernment...just because it's open-source doesn't mean it's safe. Do some due-dilligence, research, and check with Pro-Privacy groups and friends..
- For Apps that you must have, try using the *websites* instead. Facebook, Ebay, Weather apps have many trackers attached to them. Don't give up your data! :)

Phone: The standard phone App is loaded but note your conversations are NOT secure and private. *Signal* is supposedly "encrypted" and if want private conversations.

Messaging: The standard messaging App is not secure. If you want more privacy then use *Signal* and / or *Session. Session* is a very secure and anonymous App.

Email: *'/e/OS* has their own secure email system. Click on the MAIL APP icon and you can create a new email account.

- *FairEmail & K9* – These APPs are one of the options for secure email, which helps prevent "trackers". You can use most existing email to run through them. There is some setup involved. You may or may not be able to run Gmail through it.(running anything google is risky)
- *Proton & Tutanota e*mail are secure / encrypted. Both offer free & business email service. You may be able to forward your old email to newly created email. It just depends on who your current email provider is. *FairEmail* is another option for secure email, in which many existing email can run through them.
- VPN – Virtual Private Network: e/OS has a VPN has part of their ADVANCED PRIVACY feature. Swipe right and it can be seen. Better ones are Mullvad and IVPN. When used, this provides a virtual (hides) your IP address… places the location of your device, phone, tablet, PC at a different location. To use, tap on the App and choose location you want your IP address from. You can even choose a different country.

Location & Maps*:* There several great open source Map Apps. OsmAnd and Magic Earth work well. GMaps WV give many resources that Google Maps provides.
Be sure to Toggle-On the Location in quick tile settings / pull-down menu.

Backups: *Hard backup* - purchase usb C storage device (flash drive.) Plug into phone & run backup. Through "Backup" app or "Seedvault". May need format first. It will ask you first. *Cloud backup* - Seedvault is encrypted backup and restore suite. It uses Nextcloud.

Syncing: an /*e/Account* can be created upon phone startup or simply swipe right. This is their cloud in which photo's and contacts can be synced / saved.

Weather*:* App comes preinstalled or can find on Droidify/FDroid. When you open it, you will come to OWM API key a few screens later. Just do what it says to get your personal key. Feel free to use your favorites but use websites so your privacy is secure.

Newpipe / Pipepipe: 3rd party YouTube interface that allows you to watch, subscribe & even download content without a google account! It also allows you to listen to Youtube videos with the screen turned off and download Audio and/or Video.

Clouds: Mega (mega.io) is a powerful encrypted cloud service that offers files & picture syncing / sharing, private messaging, video conferencing & more!

BE PATIENT: There will be a slight learning curve with using a new operating system and striving to keep your *Privacy Freedom*. It's all worth it! Reach out to info@getprivacyfreedom.com if you need assistance and will try our best to help!