

#PAS, AOSP, FOSS: IMHO

Moisés Santos Farias

github.com/moisessmsf

moisessmsf@proton.me

Privacy, Anonymity and Security in the Android Open Source Project and its free and open source software: in my humble opinion.

Moisés Santos Farias

github.com/moisessmsf

moisessmsf@proton.me

Agenda

About me

#PAS

AOSP

FOSS

To infinity and beyond!



#PAS, AOSP, FOSS: IMHO

About me

Moisés Santos Farias

Privacy | Anonymity | SecOps

Piaçabuçu - AL

Ministério das Comunicações (MCom)

github.com/moisessmsf

moisessmsf@proton.me



#PAS

Privacy, Anonymity, Security

Privacy

- Ability to control information;
- The contents of the message can only be seen\heard by the intended recipient(s).

Anonymity

- Unknown authorship or origin, not named or identified;
- The sender and/or recipient's real ID is unknown;
- Privacy on steroids.

Security

- Freedom from danger.

EXAMPLES

1

**Security without
Privacy or
Anonymity**
(Google?)

2

**Privacy without
Anonymity (?)**

3

**Anonymity
without Security**
(Paying in the
cash?)

4

**Security and
Privacy without
Anonymity**
(Whatsapp?)

5

**Privacy without
Security or
Anonymity**
(Bathroom in the
woods?)

6

**Security with
Privacy and
Anonymity**
(XMPP?)



Threat Model



AOSP

Android Open Source Project

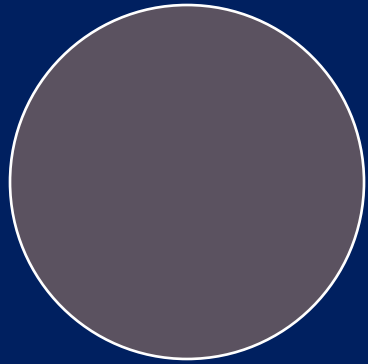
Android

Linux Kernel;
AOSP*;
Vendor Blobs;

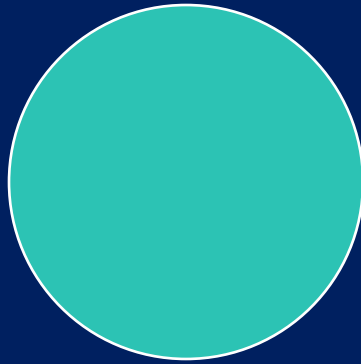
IS ANDROID #PAS?



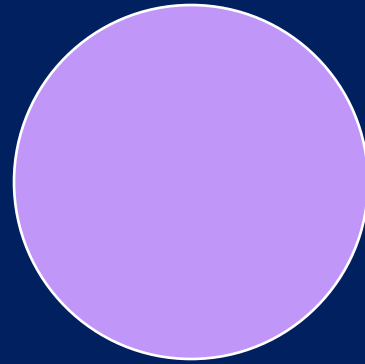
Android version



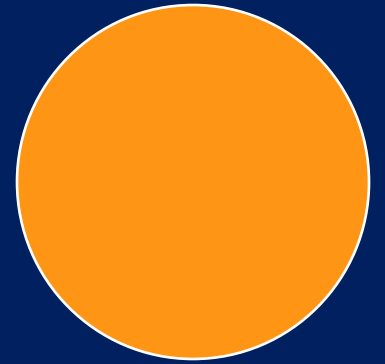
Android Security
Bulletins (ASB)



Pixel ASB



Vendor ASB



Linux kernel
version

IS ANDROID #PAS?

Google Account?

Bloatware

Discontinued devices

Insecure and proprietary blobs

Insecure bootloaders

Insecure firmware

Insecure and ancient kernels

ANDROID ROM

"Stock" ROM

- ...
- ...
- ...
- ...
- GSI (Treble)

Custom ROM Official

- LineageOS
- PixelExperience
- Evolution X
- **GrapheneOS**
- **CalyxOS**
- **DivestOS**
- ...








Custom ROM Unofficial

- ...

Comparison of Android ROMs

Source: eylenburg.github.io

Last updated: October 2023

	GrapheneOS	DivestOS	CalyxOS	IodéOS	/e/	LineageOS	"Stock" Android
							
Based on	AOSP	LineageOS	AOSP	LineageOS	LineageOS	AOSP	AOSP
Freedom							
Free and open source (FOSS)?	Yes	Yes	Yes	Yes	Yes	Yes	No
Debloated?	Yes, somewhat	Yes, extensively	Yes, somewhat	No	No	No	No
Features							
Network controls for apps	Direct and indirect access	Direct and indirect access	Direct access only	Direct access only	Direct access only	Direct access only	No
Network-based location	Emulated ^{default} , or Play Services	No	UnifiedNLP	UnifiedNLP	UnifiedNLP	No	Play Services
System-wide connection/tracker blocking	Private DNS setting, or via VPN app	hosts file, Private DNS, or VPN	Private DNS setting, or via VPN app	iodé-snort app, Private DNS, or VPN	Private DNS setting, or via VPN app	Private DNS setting, or via VPN app	Private DNS setting, or via VPN app
E2E-encrypted phone backups	Yes (Seedvault)	Yes (Seedvault)	Yes (Seedvault)	Yes (Seedvault)	Yes (Seedvault)	Yes (Seedvault)	Yes, but requires Google login
Notification forwarding from other user profiles	Yes	No	No	No	No	No	No
Android Auto compatible	No	No	No	No	No	No	Yes
Google Pay compatible	No	No	No	No	No	No	Yes
Degoogling (connections to Google)							
eSIM activation	Google EUICC (disabled by default)	OpenEUICC	Google EUICC (preinstalled)	Google EUICC (preinstalled)	Google EUICC (preinstalled)	Google EUICC (preinstalled)	Google EUICC (preinstalled)
Network location provider	Emulated/GNSS ^{default} , or Google	n/a	UnifiedNLP	UnifiedNLP	UnifiedNLP	n/a	Google
SUPL	GrapheneOS ^{default} , Google or none	Google ^{default} , or none	Google ^{default} , or none	Google ^{default} , or none	Google	Google ^{default} , or none	Google
PSDS - Google Pixel 6 and later	GrapheneOS ^{default} , Google, or none	Broadcom ^{default} , or none	Broadcom ^{default} , or none	Broadcom ^{default} , or none	Google	Google ^{default} , or none	Google
Connectivity check/captive portal	GrapheneOS ^{default} , Google, or none	Multiple presets offered	Google, but can be changed	Kuketz.de	/e/foundation	Google, but can be changed	Google, but can be changed
DNS connectivity check	GrapheneOS ^{default} , or Google	Google	Google	Google	Google	Google	Google
DNS server fallback	Cloudflare	Quad9	Cloudflare	Quad9	Google	Google	Google
Network time	GrapheneOS ^{default} , or none	NTP.org.pool and carrier-based time	Google and carrier-based time	NTP.org.pool and carrier-based time	NTP.org.pool and carrier-based time	Google and carrier-based time	Google and carrier-based time
Hardware attestation provisioning	GrapheneOS ^{default} , or Google	Google	Google	Google	Google	Google	Google
Google Play Services							
Implementation	Sandboxed Play Services (optional)	Unprivileged microG (optional)	Privileged microG (optional)	Privileged microG (optional)	Privileged microG	None by default. It's possible to add Google Apps manually during the installation process, but this is not officially supported by LineageOS.	Privileged Play Services
FOSS? (see tooltips for details)	Google binaries in FOSS sandbox	Yes, but executes proprietary code	Yes, but executes proprietary code	Yes, but executes proprietary code	Yes, but executes proprietary code	Alternatively, there is the LineageOS for microG project that integrates microG in LineageOS.	No
Sandboxed/unprivileged?	Yes	Yes	No	No	No		No
Can be limited to work profile?	Yes	Yes	No	No	No		No
Signature spoofing needed/allowed?	No	Only for Google signature	Only for Google signature	Allowed for any app & signature	Allowed for any app & signature		No
Push notifications via Google FCM?	Yes	Optional	Optional	Optional	Optional		Yes
Can deny FCM registration for specific apps?	No	Yes	Yes	Yes	Yes		No
Google Play Integrity/Safetynet?	Yes	No	Yes	Yes	Yes		Yes
Privacy							
Storage scopes	Yes, see here	No	No	No	No	No	No
Contact scopes	Yes, see here	No	No	No	No	No	No
Per-app sensor controls	Yes	Yes	No	No	No	No	No
Per-connection DHCP state flushing	Yes	Yes	No	No	No	No	No
Per-connection MAC address randomization	Yes	Yes	No	No	No	No	No
SUPL: IMSI or phone number sent?	No	No	No	No	Yes	No	Yes
PSDS: user agent sent?	No	No (device-specific), see here	Partially for Qualcomm chips	for Qualcomm GPS chips	for Qualcomm GPS chips	Partially for Qualcomm chips	for Qualcomm GPS chips
Closed cross-profile package leaks?	Yes	Yes	No	No	No	No	No
Closed device identifier leaks?	Yes, see here	No	No	No	No	No	No
Metadata stripping for screenshots/photos	Yes	No	No	No	No	No	No

#PAS TO ANDROID(?)

Avoid Rooting

Google Account?



Install Updates

Review Permissions

Encryption

Uninstall or disable apps

Replace apps



Screen lock



#PAS, AOSP, FOSS: IMHO

WAYDROID

Full Android on GNU/Linux

LineageOS

(without GAPPS or with GAPPS)

GPL-3.0

<https://waydro.id/>

<https://github.com/waydroid/waydroid>



#PAS, AOSP, FOSS: IMHO

A large light blue circle is centered on a dark blue background. A dashed teal line arcs from the top left towards the circle. A small purple circle is located at the bottom right edge of the light blue circle.

Threat Model



FOSS

Free and Open Source Software

SECURITY, PRIVACY AND ANONYMITY THROUGH FOSS APPS IN ANDROID IN MY HUMBLE OPINION*

Neo Store

F-Droid client
GPLv3



<https://github.com/NeoApplications/Neo-Store/>

20 Software
YEARS Freedom Day

#PAS, AOSP, FOSS: IMHO

Aurora Store

Google Play Store client
Anonymous accounts
GPLv3



<https://auroraoss.com>
<https://gitlab.com/AuroraOSS/AuroraStore>

20 Software
YEARS Freedom Day

#PAS, AOSP, FOSS: IMHO

Simple Mobile Tools

File Manager, Gallery,
Calendar, Contacts, SMS,
Keyboard, etc...

Without ads or unnecessary
permissions

GPLv3



<https://www.simplmobiletools.com>
<https://github.com/SimpleMobileTools>

 **20** Software
YEARS Freedom Day

#PAS, AOSP, FOSS: IMHO

KDE Connect

Integration between devices
Remote control, notifications,
share files, links, clipboard, ...
GPLv3



<https://userbase.kde.org/KDEConnect>
<https://github.com/KDE/kdeconnect-kde>

20 Software
YEARS Freedom Day

#PAS, AOSP, FOSS: IMHO

Authpass

Password Manager
Multiplatform
Offline & Cloud
Compatible with KeePass
GPLv3



<https://authpass.app>
<https://github.com/authpass/authpass>

20 Software
YEARS Freedom Day

#PAS, AOSP, FOSS: IMHO

DroidFS

Encrypted storage

GoCryptFS

Internal support for video, audio
images, text and PDF files

AGPLv3



<https://forge.chapril.org/hardcoresushi/DroidFS>
<https://github.com/hardcore-sushi/DroidFS>

20 Software
YEARS Freedom Day

#PAS, AOSP, FOSS: IMHO

Syncthing

Continuous File Synchronization
Multiplatform
Private and Secure
MPLv2



<https://syncthing.net>
<https://github.com/syncthing>

20 Software
YEARS Freedom Day

#PAS, AOSP, FOSS: IMHO

Orbot/ Tor Browser

Anonymity (?)

Tor or "VPN" full device or per
app

BSD-3-Clause



<https://www.torproject.org/download/#android>
<https://github.com/guardianproject/orbot>

20 Software
YEARS Freedom Day

#PAS, AOSP, FOSS: IMHO

Wireguard

Modern and fast VPN protocol

VPN full device

GPLv2, Apache-2.0



<https://www.wireguard.com>

<https://git.zx2c4.com/wireguard-android>



#PAS, AOSP, FOSS: IMHO

Rethink DNS

DNS + Firewall + VPN + Tor +
SOCKS5 + Content blocking +
Network monitor
Apache-2.0



<https://rethinkdns.com/app>
<https://github.com/celzero/rethink-app>

20 Software
YEARS Freedom Day

#PAS, AOSP, FOSS: IMHO

Monerujo

Monero means money!

Confidential, untraceable,
private and censorship-
resistant cryptocurrency

Apache-2.0

<https://www.monerujo.io>
<https://github.com/m2049r/xmrwallet>



20 Software
YEARS Freedom Day

#PAS, AOSP, FOSS: IMHO

Mull Browser

Privacy hardened Firefox-based
AGPL-3.0



https://divestos.org/pages/our_apps#mull
<https://github.com/Divested-Mobile/mull-fenix>

20 Software
YEARS Freedom Day

#PAS, AOSP, FOSS: IMHO

Instant Messaging

SimpleX Chat

E2E + Incognito mode + no ID

Relay servers

AGPL-3.0



<https://simplex.chat>

<https://github.com/simplex-chat/simplex-chat>



#PAS, AOSP, FOSS: IMHO

Instant Messaging

<https://matrix.org>
<https://github.com/matrix-org>

Matrix (Schildchat\Element)
E2E + Federated + Bridges
Apache-2.0



#PAS, AOSP, FOSS: IMHO

APPS

Neo Store, Aurora Store

Simple Mobile Tools

KDE Connect

Authpass

DroidFS

Syncthing

Orbot\Tor Browser

Wireguard

RethinkDNS

Monerujo

Mull Browser

SimpleX Chat, Matrix

Telegram, Whatsapp

Standard Notes

Google Maps

Mulch

Colabora Office

Termux

VLC

Proton Mail, Tutanota

...



#PAS, AOSP, FOSS: IMHO



Threat Model

MORE OPINIONS

Privacy Guides

<https://www.privacyguides.org/en/tools/>

<https://discuss.privacyguides.net/>

Eylenburg

<https://eylenburg.github.io>

Awesome Privacy lists

<https://github.com/pluja/awesome-privacy>

<https://github.com/Lissy93/awesome-privacy>

Privacy Tests

<https://privacytests.org>

Techlore

<https://discuss.techlore.tech/>

<https://www.techlore.tech/spa>

<https://www.techlore.tech/resources>

The New Oil

<https://thenewoil.org>

DivestOS

https://divestos.org/pages/recommended_apps

<https://divestos.org/pages/browsers>

<https://divestos.org/pages/messengers>



#PAS, AOSP, FOSS: IMHO

TO INFINITE AND BEYOND!

DNS

- DoH, DNSCrypt
- ODoH
- DoOH
- MODoH

HTTP

- QUIC, HTTP3
- OHTTP

TLS

- ECH



Thanks!

Moisés Santos Farias

github.com/moisessmsf

moisessmsf@proton.me



#PAS, AOSP, FOSS: IMHO