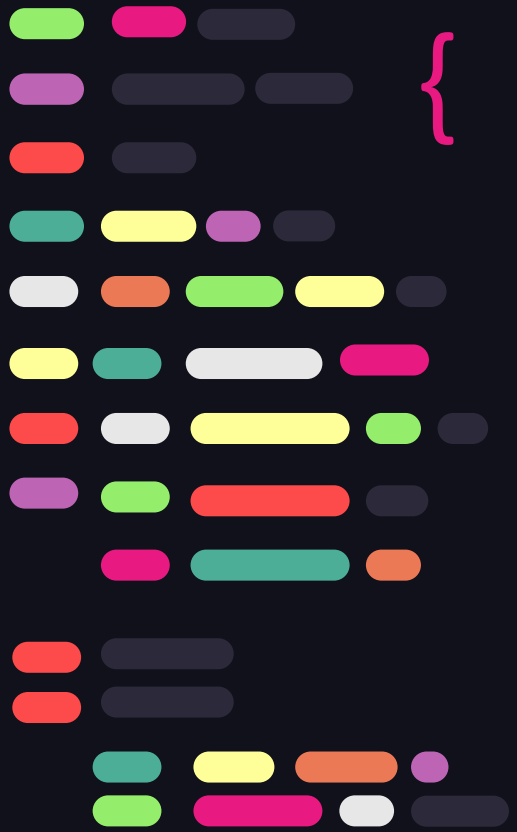


Introduction to GrapheneOS

a fork of Android AOSP

Series: OSSFTW (Open Source Software For The Win!)

Table of contents

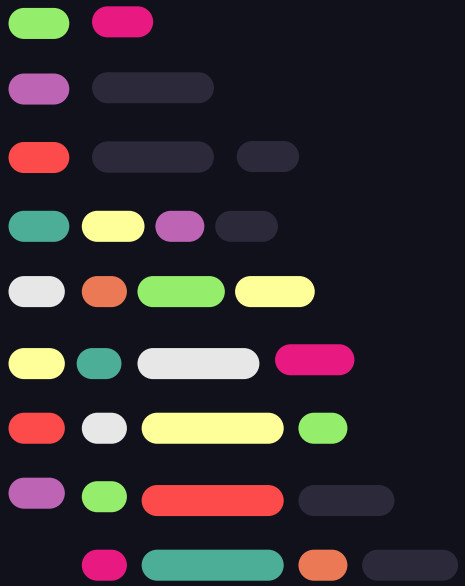
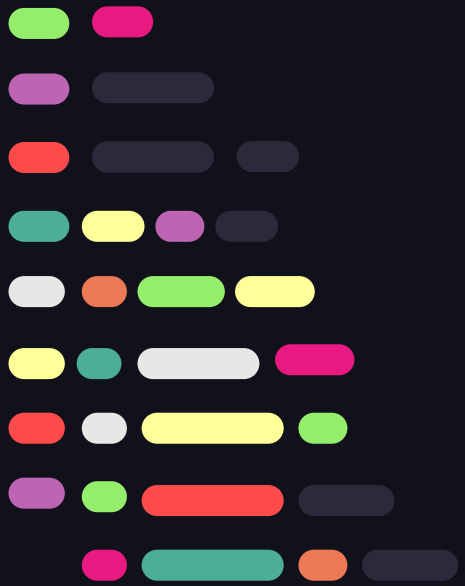
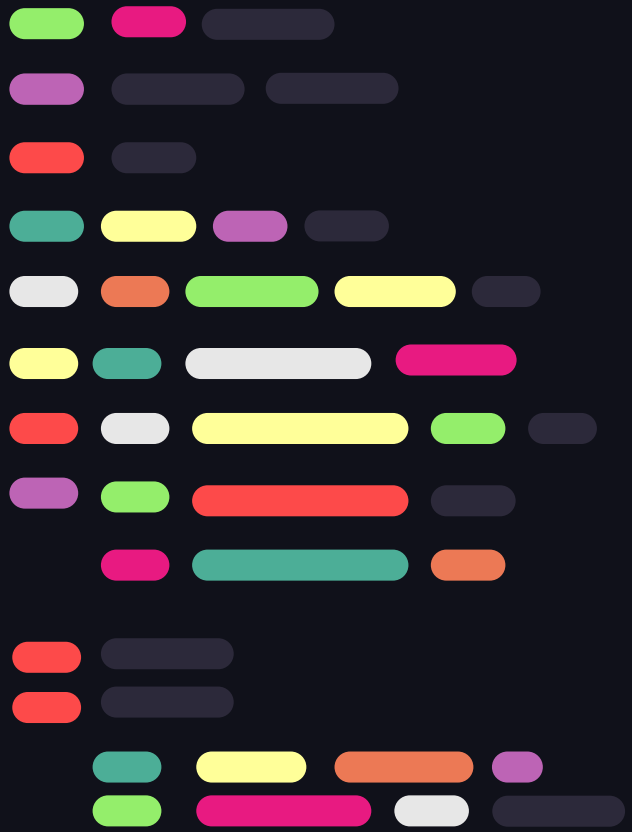


Table of contents

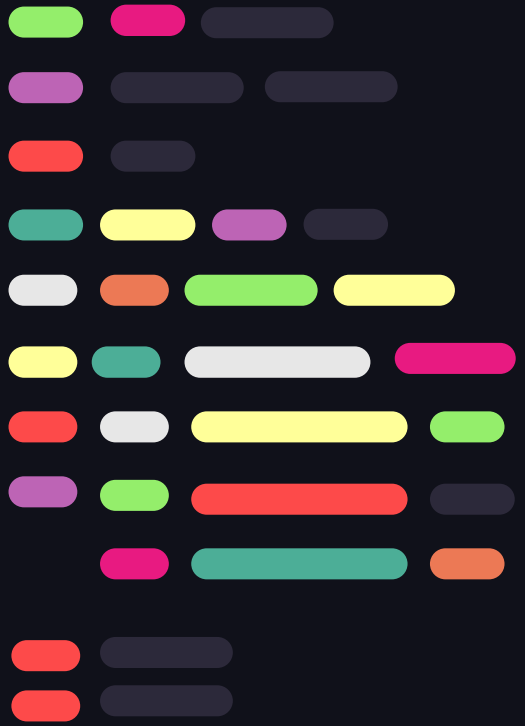




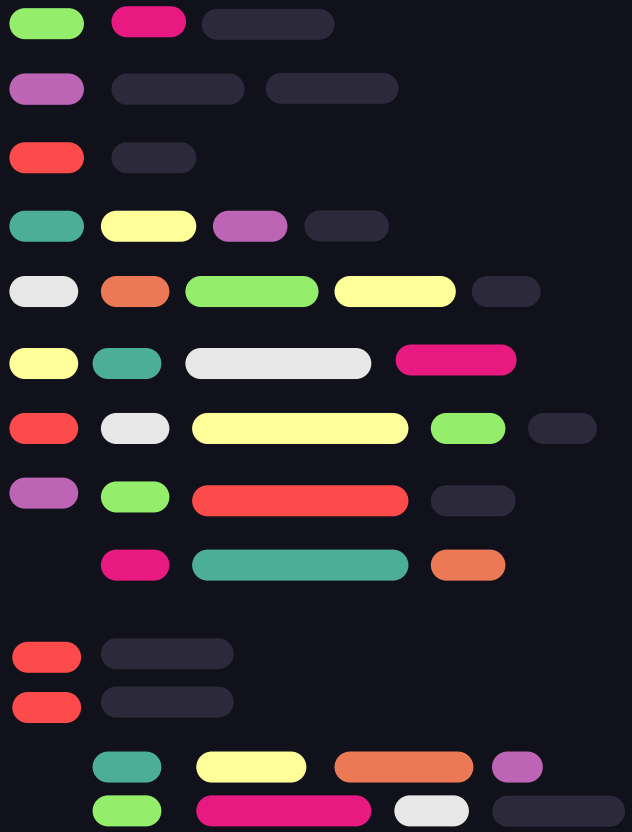
I have Nothing to Hide

... and everything to lose!

Loss of Civil Liberties



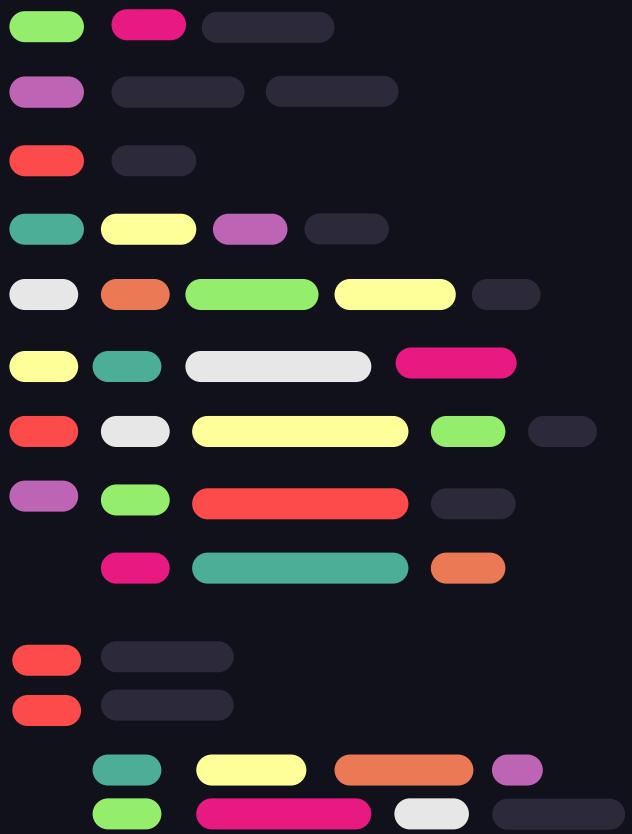
- Wrongful Arrests: Man wrongfully goes to Prison for Murder based on Google's Geo-Fence data (Wired)
- **Stalking:** Facebook Employee misuses private data to Stalk a Woman (Guardian)
- Data Breaches: Cambridge Analytica, stole and sold data from 50-90 million Facebook users for Election Rigging (Guardian)
- Changing Laws (Roe v Wade): Woman indicted for searching "Abortion Pills" (Guardian)
- State Oppression: Biometric Recognition Systems, Human Rights violation & targeting of journalists, dissidents, etc. (UN Report)



The “Data Freedom” Movement

... and other growing pains


They see everything… (@christitustech)



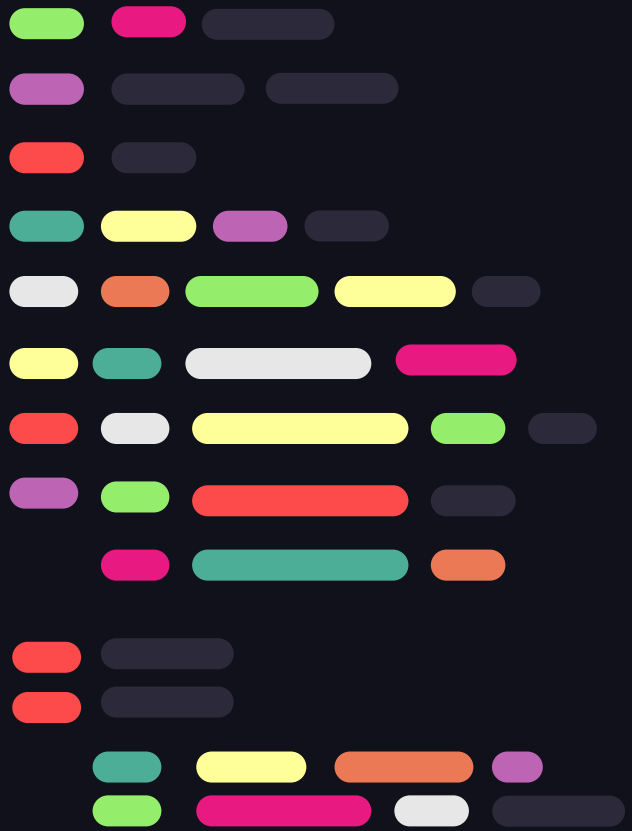
{ How will you be paying tonight:

Cash,
Credit,
or Data?

JK, we'll take your data either way }

Privacy vs Security

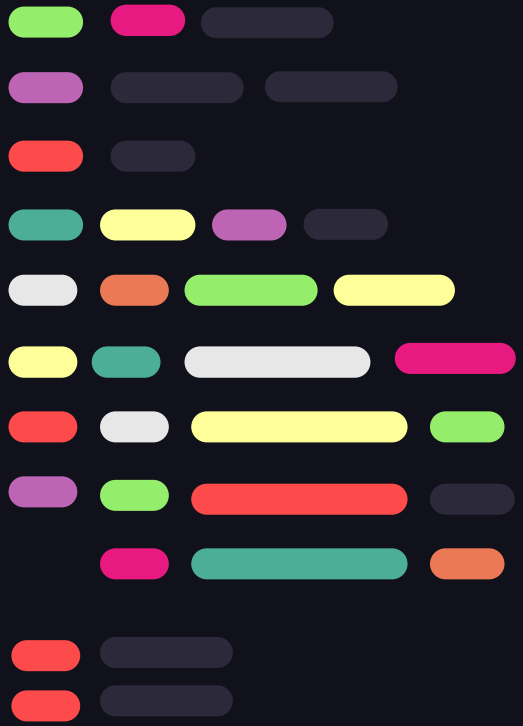
Privacy	Security
Minimize Data Collection	Maximize Data Protection
Proper usage, processing, and storage of data	Protect against malware, hacks, and breaches
E.g., Aliasing, Encryption, etc.	E.g., 2FA, Security Patches, etc.



Privacy Threat Models

- Life-Threatening (Snowden)
- Freedom of Speech (Journalists, etc.)
- Vulnerable Segments (ethnic minorities)
- Domestic Abuse Victims
- Anti-Big Tech Surveillance
- Two-Day Battery Club

Privacy threat Categories



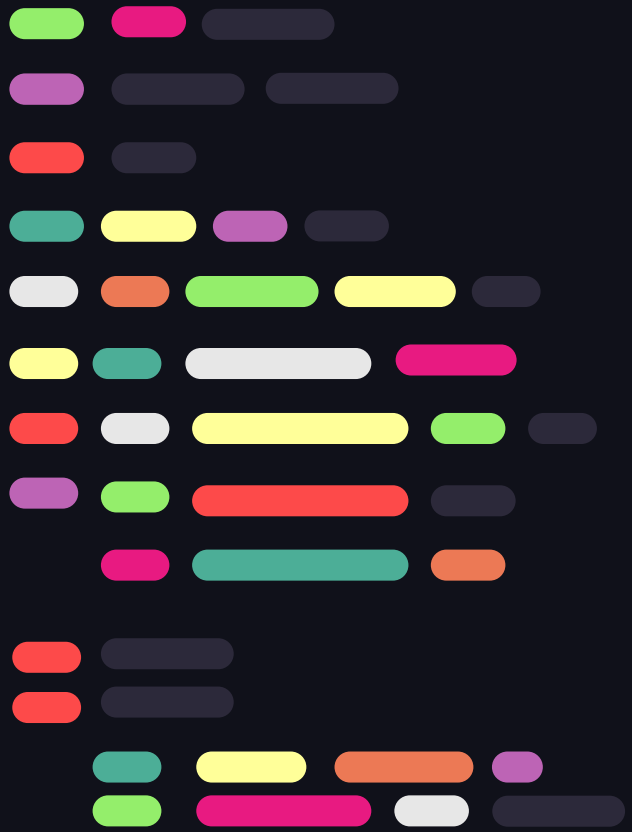
Who you are (identifiers) +
What you do (activity trail)

- Linkability
- Identifiability
- Detectability
- Disclosure of Information
- Unawareness
- Etc.

https://codific.com/privacy-threat-modeling/

https://ssd.eff.org/module/your-security-plan

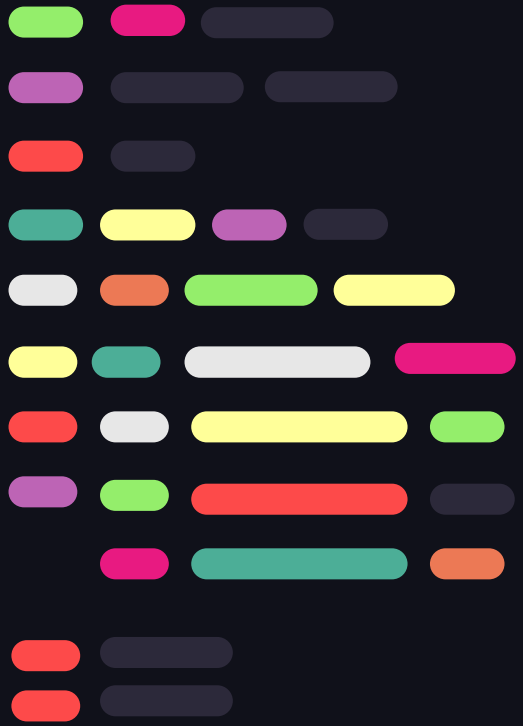
https://www.privacyguides.org/en/basics/threat-modeling/#try-it-yourself-protecting-your-belongings



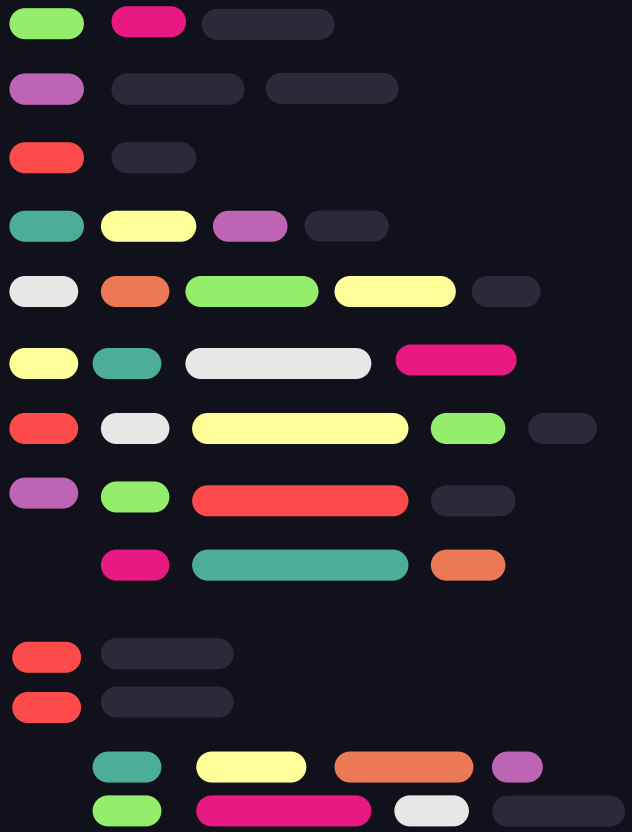
Privacy through Operational Security (OpSec)

... minimizing the attack surface.

Privacy through OpSec



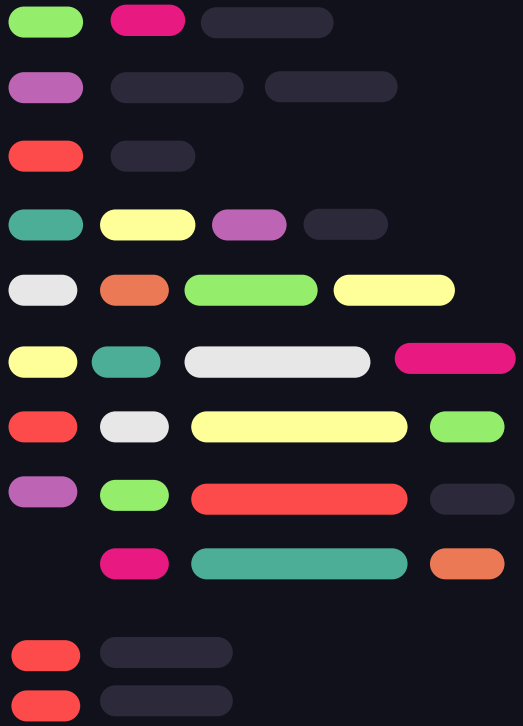
- Isolate Mobile Devices
- Browser Isolation
- Use Hardened Browsers (Vanadium, Mull, Mullvad Browser, LibreFox, etc.)
- Content Filtering (uBlock Origin)
- Encrypted DNS (Ad-Guard, Quad9, NextDNS)
- VPNs or TOR/Onion
- Compartmentalize Work/Personal/Financial data
- Use Pseudonyms
- Data Poisoning
- Temporary Email IDs
- Email Aliases (addy.io, SimpleLogin, etc.)
- Phone Aliases (VoIP, MySudo, etc.)
- Masked Payment (Privacy.com, Apple Pay, etc.)



GrapheneOS Security Features

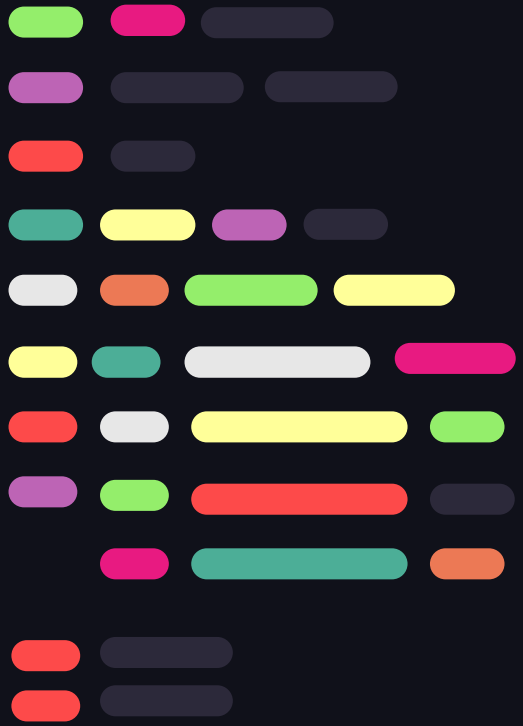
... and what you'll miss vs. the Stock OS

Security Features

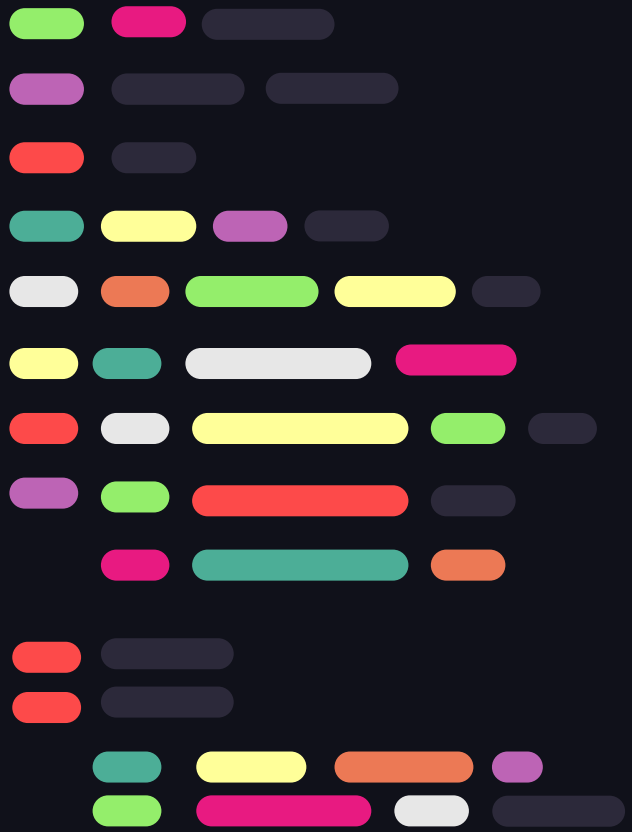


- Verified Boot ensures all executed code comes from a trusted source, such as GrapheneOS. It establishes a full chain of trust from the hardware to the software (for Tamper Protection).
- Disable Native Code Debugging to improve application sandboxing. This can interfere with apps debugging their own code to add a barrier to analyzing the app (hence some banking apps require this to be enabled).
- Secure App Spawning disabling apps from sharing the same initial memory content and layout for stronger app and user profile sandboxing (link)

Security Features



- **Site-Level Sandboxing in Vanadium Browser.**
- **Auto Reboot** to put the device **fully at rest** (disabling biometrics, notification and data access until manually unlocked)
- **Sandboxed Google Play Services** (as opposed to insecure third-party app stores) using a compatibility layer to **disable privileged access**, while still using first party store.

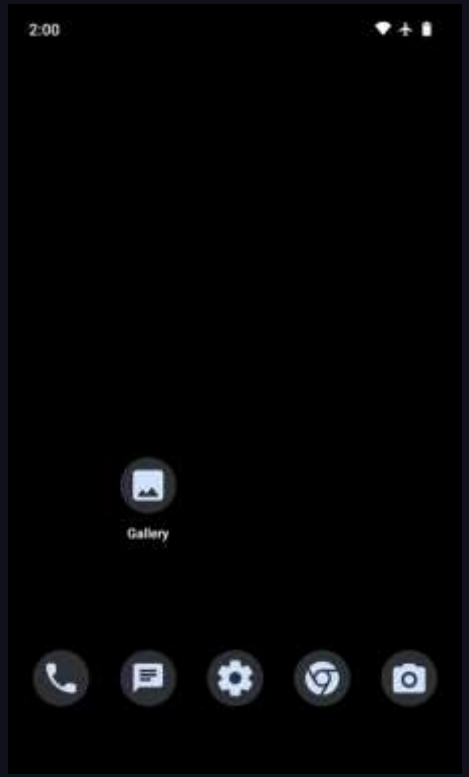


GrapheneOS Privacy Features

... and what you'll miss vs. the Stock OS

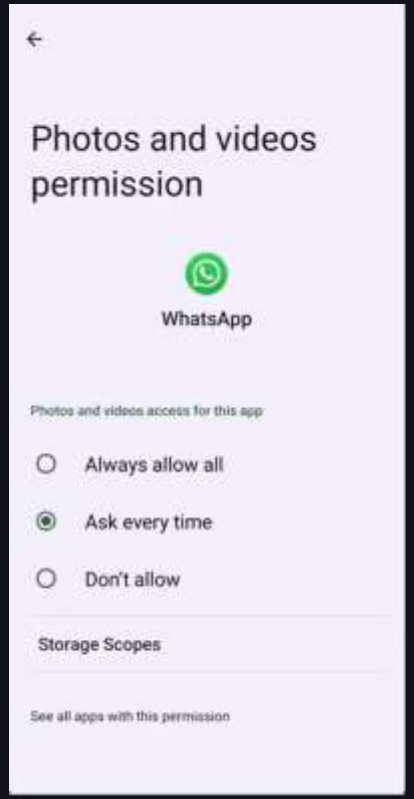
Debloated for a Smaller Attack Surface

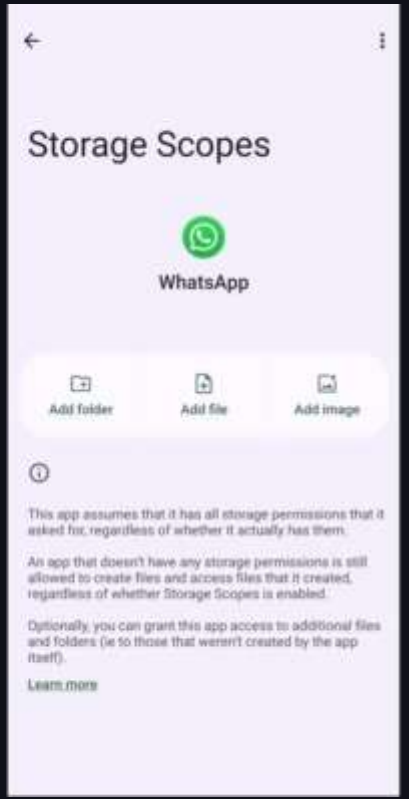
GrapheneOS comes with only the minimal required, open source apps.



Storage Scopes

Storage Scopes spoofs “All Files Access” Permission required by apps, optionally giving access to specific files or folders. Apps can still access files they create themselves.



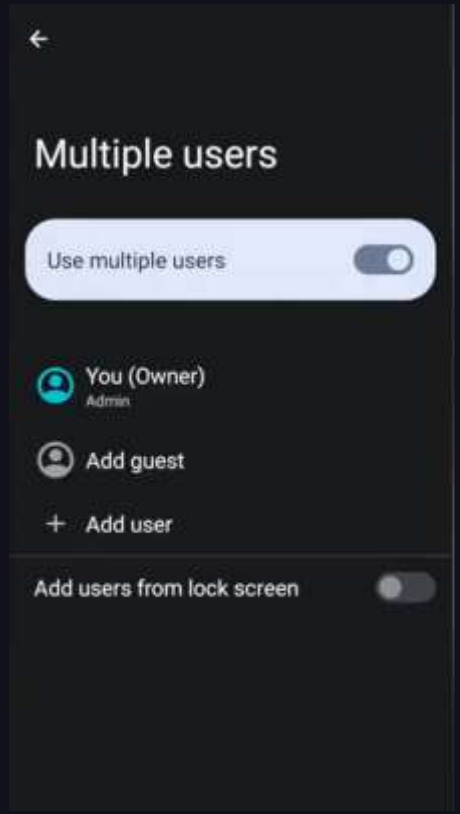


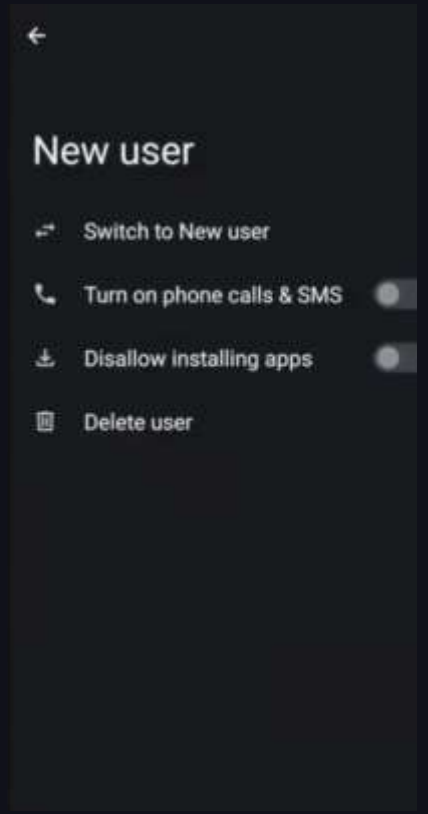
Contact Scopes

Contact Scopes spoofs “Contacts” Permission required by apps, optionally giving access to specific contacts or groups.

Sandboxed User Profiles

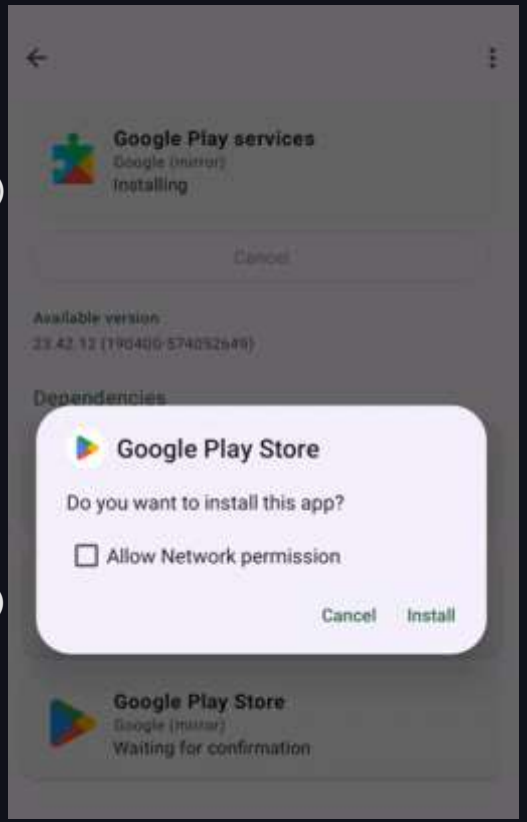
User Profiles help create upto 32 sandboxed virtual environments, while limiting access to permissions like Calls & SMS, App Installation, Run in Background, Cross-Profile Notifications, etc.



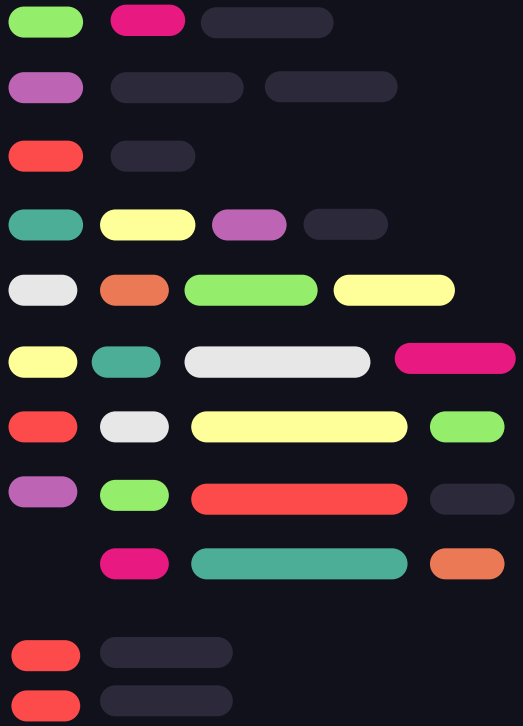


Miscelleneous Features

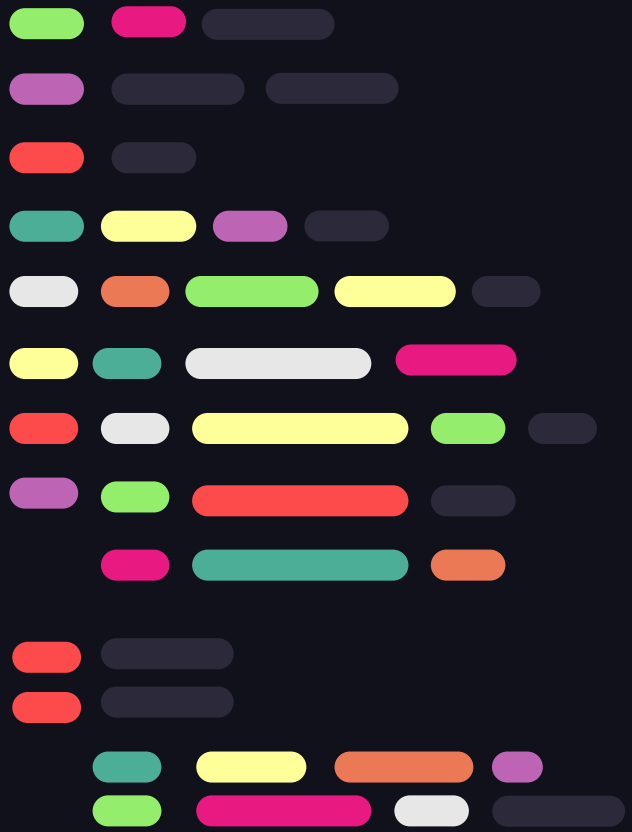
- Disable Network before or after installing an app
- Disable Apps without uninstalling them
- Disable SIM Card when not in use
- Device Identifier Obfuscation (IMEI, IMSI, WiFi MAC, etc.)
- Turn Off WiFi/ Bluetooth Automatically: reduces attack surface, stops device ID broadcasts, protects against sniffing devices (e.g., in super markets).
- Encrypted DNS (AOSP Feature).
- Always ON VPN **by default.**
- **Disable unwanted** Wireless Emergency Alerts**.**
- PIN Scrambling **for shoulder surfing attacks.**
- Google Cloud Messaging **(optionally on a secondary profile) through sandboxed play services**



Stock OS Feature You'll Miss (maybe)



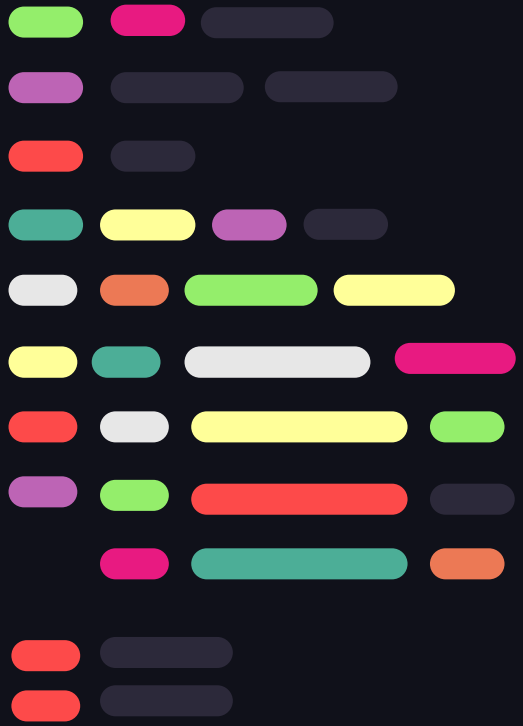
- On-Device Customization Learning (smart replies, etc.)
- On-Device Gemini Nano AI (Pixel 8 onwards)
- AI-generated wallpapers
- Call Screening / Hold For Me (US only)
- Live Captions
- Live Transcribe



UpStream Contributions

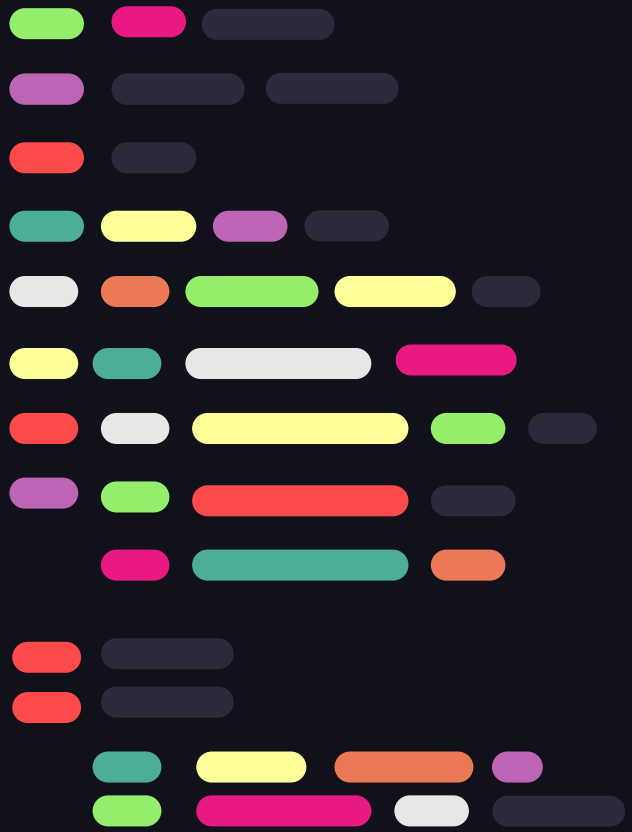
... to Billions of devices.

Upstream Contributions



Contributions to the privacy and security of the following projects gives credibility to the GrapheneOS community.

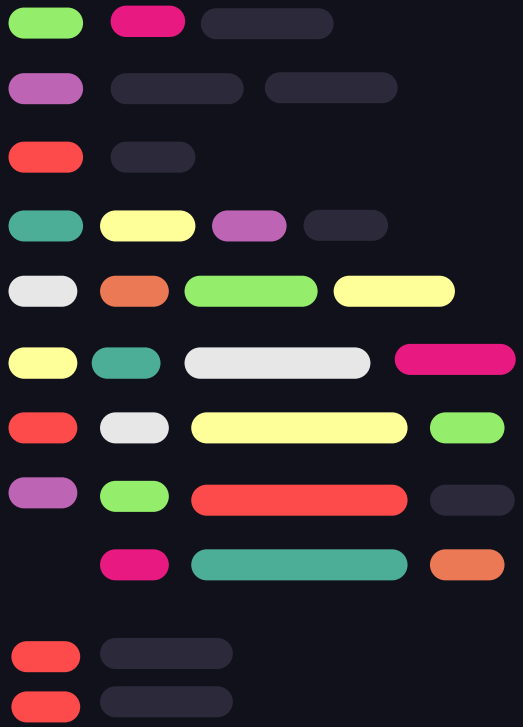
- Android Open Source Project (AOSP)
  (e.g., removing app access to:
  low-level process,
  network,
  timing and
  profiling information).
- LLVM
- Linux kernel
- OpenBSD



Installation Guide

... and how to revert to Stock OS.

Selecting a Device



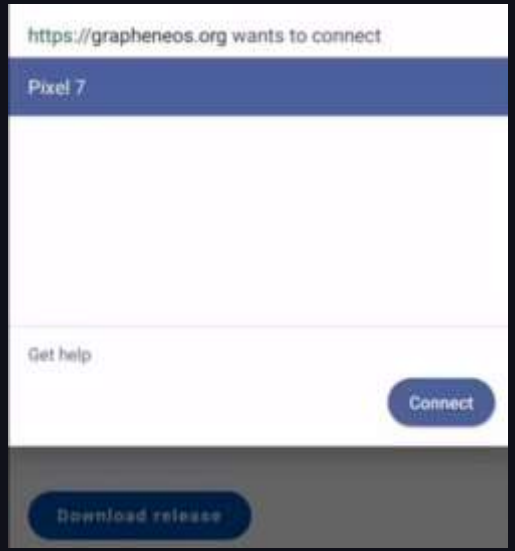
Device	OEM support end date	OEM support
Google Pixel 8 Pro	October 2030	7 years
Google Pixel 8	October 2030	7 years
Google Pixel Fold	June 2028	5 years
Google Pixel Tablet	June 2028	5 years
Google Pixel 7a	May 2028	5 years
Google Pixel 7 Pro	October 2027	5 years
Google Pixel 7	October 2027	5 years
Google Pixel 6a	July 2027	5 years
Google Pixel 6 Pro	October 2026	5 years
Google Pixel 6	October 2026	5 years
Google Pixel 5a	August 2024	3 years

****Check “Enable OEM Unlocking” setting for a carrier-unlocked device****

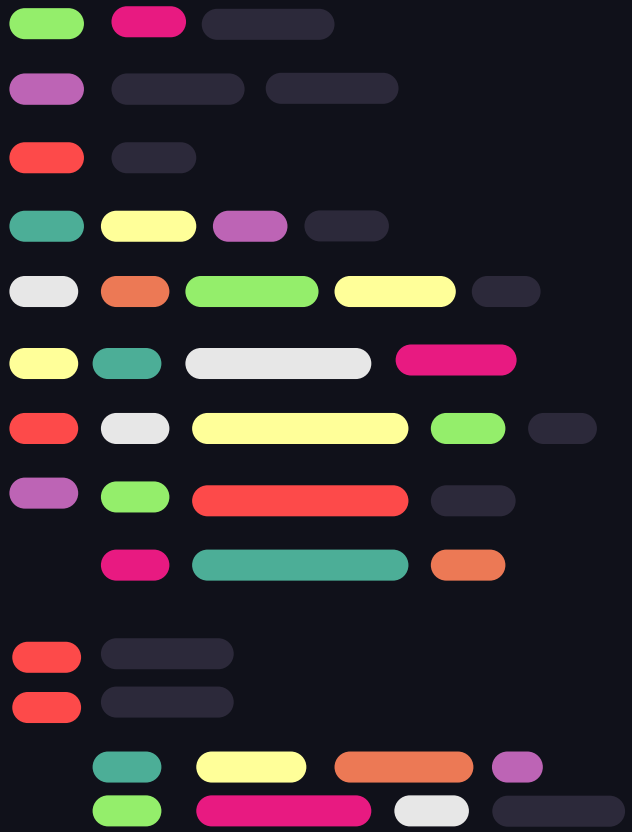
https://grapheneos.org/faq#supported-devices

https://grapheneos.org/faq#device-lifetime

Step-by-Step Web Installer

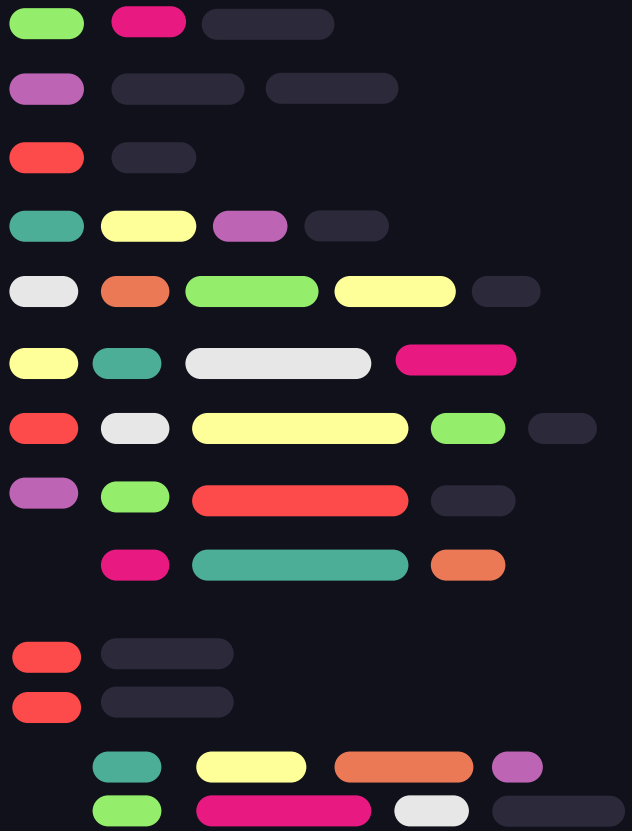


Web Installer: https://grapheneos.org/install/web
Desktop Web Installer (Video): https://yewtu.be/watch?v=ZAZlmYKrwfk
Mobile Web Installer (Video): https://yewtu.be/watch?v=b4liuCRRjH0
CLI Installer (Advanced): https://grapheneos.org/install/cli



Honorable Mentions

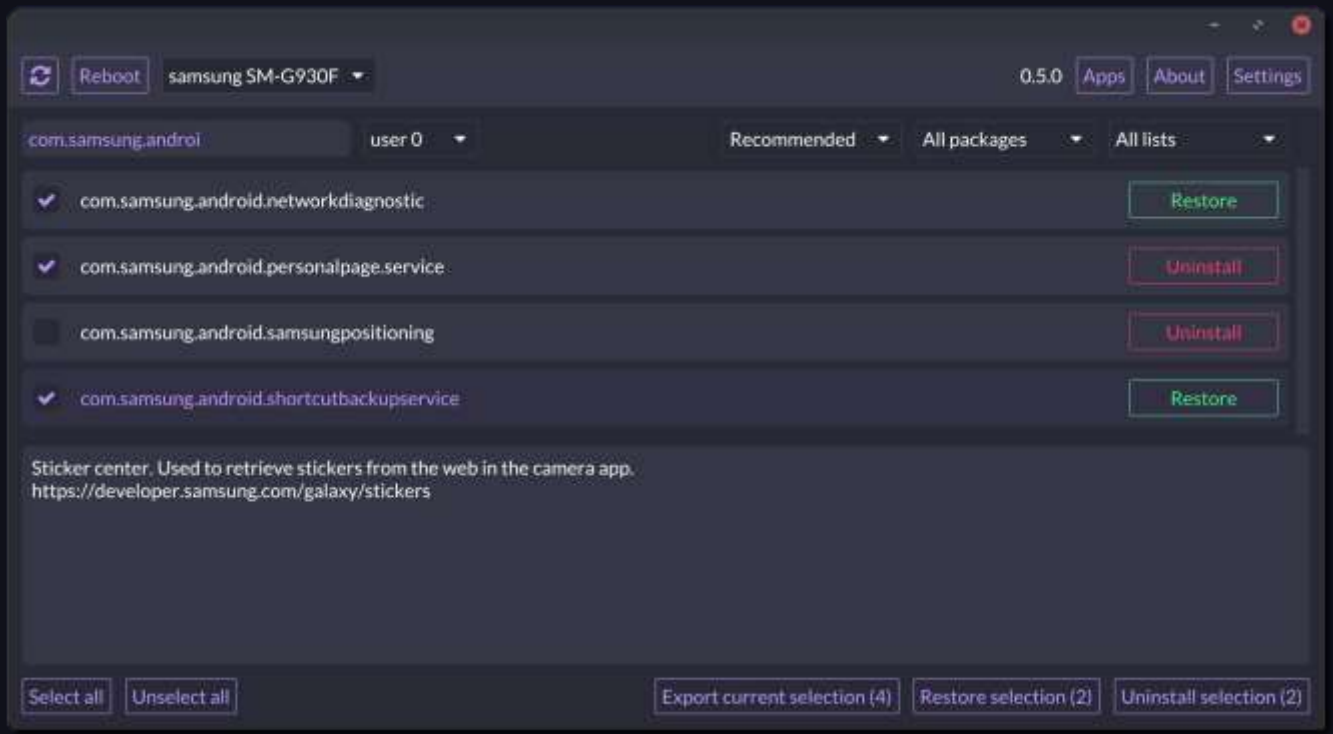
... CalyxOS, DivestedOS, e/ OS, F-Droid, Aurora Store and MicroG.



Debloating an Unsupported Android Device

... Using the Universal Android Debloater

Debloating an Unsupported Android Device



Universal Android Debloater:
https://github.com/0x192/universal-android-debloater

Resources

- https://grapheneos.org/
- https://grapheneos.org/usage
- https://discuss.grapheneos.org
- https://github.com/grapheneos
- https://github.com/tycrek/degoogle
- https://www.privacytools.io
- https://www.privacyguides.org/en/
- https://surveillancereport.tech
- [Book] Extreme Privacy: Mobile Devices - by Michael Bazzell

Thanks!

< Where can you find me >

Github.com/QuillPusher

linkedin.com/in/QuillPusher/

CREDITS: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon**, and infographics & images by **Freepik**