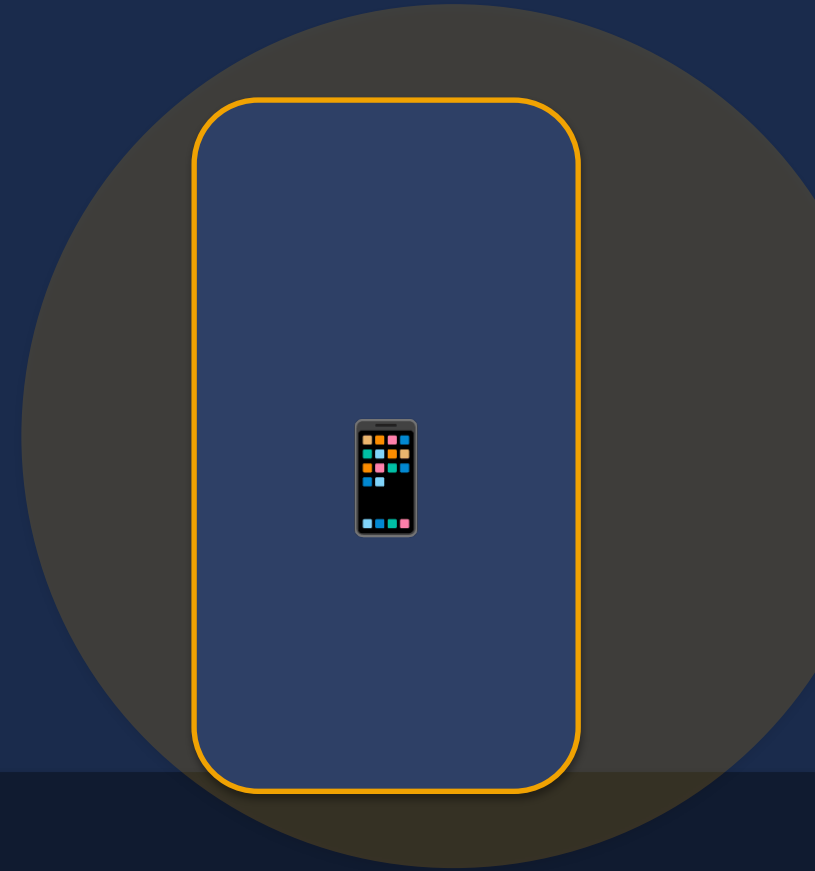


#DEGOOGLIFYANDROID · FSMI



Degooglify Android

Free Android, Free your Mobile Device

- Your phone. Your rules.
- 750 million Indians. One default.

THE NUMBERS

India's Android Reality, Google's Grip



INDIA'S ANDROID REALITY

95%+

of Indian smartphones run Android

~1B

smartphone users expected in India by 2026

18B

app downloads on India's Play Store in 2025 — 22% of all Play downloads, worldwide



GOOGLE'S GRIP ON INDIA

94%

of Indian search traffic goes through Google

~90%

Chrome share of Indian browsers — highest of any large country

518M

Indians on YouTube — its single largest market, worldwide

One company. Nearly every layer. That's the monopoly this campaign is about.

THE HOOK

Your Phone Reports Every 15 Minutes

- Location. Search. YouTube. Logged constantly.
- You never explicitly agreed to this.
- It happens quietly, in the background.
- This isn't a Google-hate slide.

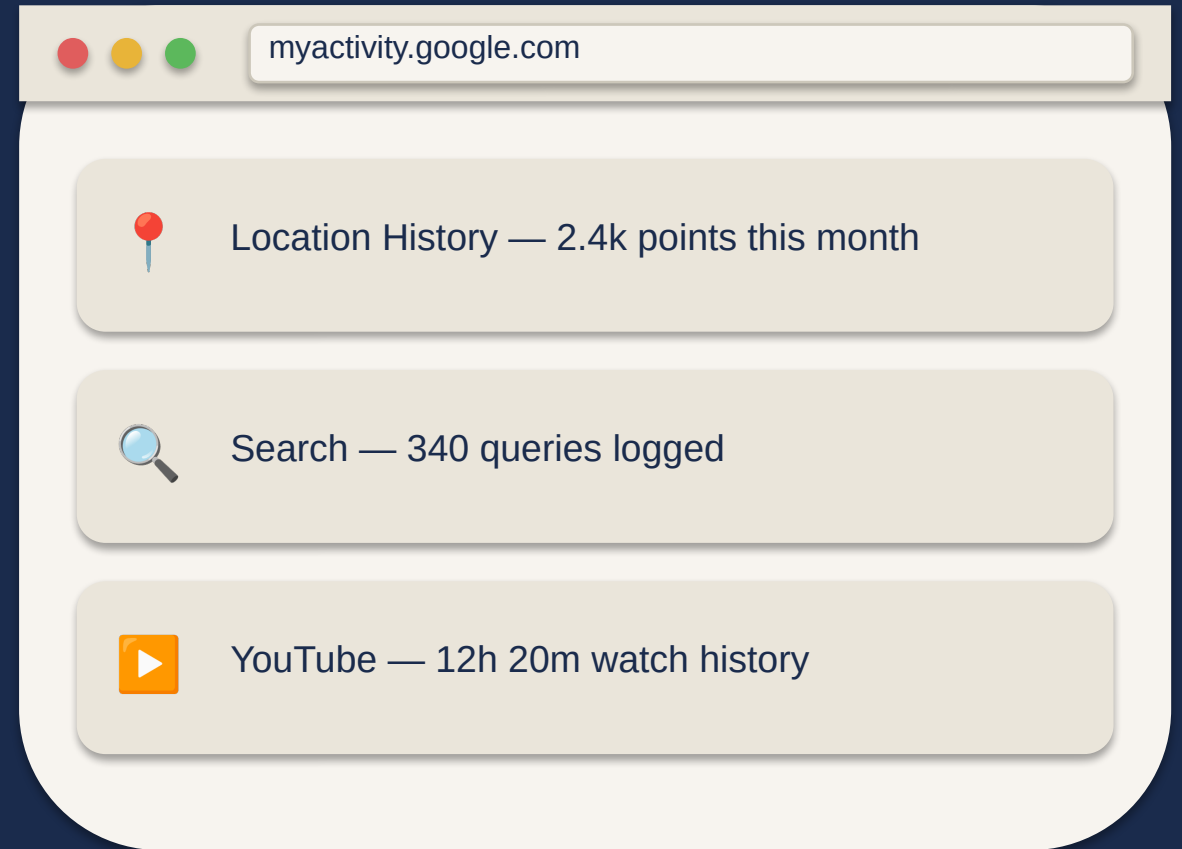
15

MINUTES, ON AVERAGE

LIVE DEMO

See It For Yourself

- Live: myactivity.google.com, right now.
- This is a real account's history.
- Scroll: location, searches, watch history.
- Ask: did you consent to this?



IT'S NOT JUST WHAT — IT'S HOW MUCH

More Data Than You'd Guess

340

location pings sent in 24 hours — from a phone just sitting still, screen off, nothing opened.

11.6 MB

sent to Google's servers per day with zero active use — about 0.35 GB a month before you've touched anything.

AND IT'S NOT VAGUE

This isn't “you were near a mall.” It's GPS-precise coordinates, timestamped to the second, cross-referenced with every other signal your phone sends that day.

WHERE DOES ALL THIS GO?

The Auction You Never Agreed To

- Every time an ad loads on your phone, a real-time auction runs — in under 100 milliseconds.
- 178 trillion bid requests happen globally every year — ~91% of display ads work this way.
- Only ONE company wins the ad slot. Every company that bid already received your data — device ID, IP, GPS location, browsing history — win or lose.
- Even the ad industry's own trade body (IAB Europe) admitted in writing to EU regulators that this system is “incompatible” with real consent.

This is what “surveillance capitalism” means in practice: your behavior isn't just watched. It's auctioned — thousands of times a day — to companies you've never heard of.

HISTORICAL PRECEDENT

This Isn't Hypothetical

- Edward Snowden reveals PRISM — an NSA program tapping data from Google, Microsoft, Yahoo, Apple.
- Legal basis: FISA Section 702 compels compliance; gag orders bar companies from disclosing requests.
- Google confirmed complying with lawful government data requests under this framework.
- This wasn't a hack. It was the law, working exactly as designed.

2013

THE PRISM LEAKS

WHY THIS MATTERS BEYOND PRIVACY

The CLOUD Act & Digital Sovereignty

- The US CLOUD Act lets US agencies compel Google to hand over data stored anywhere — overriding local law.
- Your Gmail, Drive, Location History sit on Google's servers — under US jurisdiction, not India's DPDP Act, 2023.
- Digital sovereignty: control over your citizens' data, infrastructure, and software — not another nation's default.
- For India & the Global South: dependency on US-run infrastructure means dependency on US law, courts, and interests.

2018

THE US CLOUD ACT

THE REFRAME

Android Is Free. Google Isn't.

- Android core (AOSP) is open source.
- Google adds a proprietary layer on top.
- That layer is what tracks you.
- You can keep Android, drop the layer.



Google Services

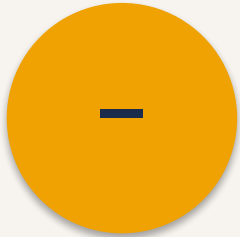
tracking, ads, lock-in

AOSP / Android

open source, yours to keep

THE PATH

Reduce, Replace, Reclaim



Reduce

Turn off what you can.



Replace

Swap apps, keep function.



Reclaim

Go further, when you're ready.

No step is mandatory past step one.

THE MENU

Top 10 Google Apps, Two Ways Out

GOOGLE APP	CLIENT-ONLY FOSS / CONTAINERISED	FULL FOSS ALTERNATIVE
Chrome	—	Chromium / Firefox
YouTube	NewPipe / LibreTube	PeerTube
Gmail	Thunderbird (your Gmail account)	Thunderbird (riseup.net or similar)
Google Maps	Containerised (Shelter work profile)	Organic Maps / OsmAnd
Google Photos	Containerised (Shelter work profile)	Nextcloud / Immich
Google Drive	Containerised (Shelter work profile)	Nextcloud
Google Calendar	DAVx5 (synced to Google)	Etar + Nextcloud Calendar
Google Search	—	SearXNG
Google Keyboard	—	FlorisBoard / IndicKeyboard
Play Store	Aurora Store	F-Droid

YOUR PACE

Three Levels, Your Choice

Level 1: Clean Up

Thirty minutes, zero risk.

1

Level 2: Break Dependency

Needs some confidence.

2

Level 3: Liberate

Full custom ROM, optional.

3



LEVEL 1

Clean Up

30 minutes · Zero risk · No root

- Install F-Droid, then Firefox + Organic Maps + NewPipe + FlorisBoard.
- Add Aurora Store — Play Store apps via anonymous login, no Google account.
- Change default apps: Settings → Apps → Default Apps.
- Pause & delete history at myactivity.google.com.
- Nothing is deleted, nothing breaks — fully reversible anytime.

LEVEL 1 • STEP-BY-STEP

Stop the Leaks

You don't have to delete your Google account. Just make it stop tracking you.

- ✓ Web & App Activity — turn OFF, delete old activity.
- ✓ Location History — turn OFF.
- ✓ YouTube History — turn OFF.
- ✓ Ad Personalization — turn OFF.
- ✓ Advertising ID — delete it (Settings → Google → Ads).
- ✓ Usage & Diagnostics — OFF.
- ✓ Google Location Accuracy — OFF (Maps still works via GPS, slightly slower lock).

Path for all of this: Settings → Google → Manage your Google Account → Data & Privacy.

LEVEL 1 · BE PRACTICAL

What to Keep — The Indian Essentials

UPI / Banking

Prefer BHIM (NPCI) — a direct, Google-free UPI option. GPay, PhonePe, Paytm need Play Services if you keep them.

UMANG / IRCTC

Keep. These need Play Services — install via Aurora Store (next slide) for a Google-account-free path.

WhatsApp

Keep (consider Signal for friends/family). Switch Google Drive backup to OFF or local.

Google Maps

Use Organic Maps or OsmAnd (OSM) first. Need live metro traffic? Run GMaps containerised (Shelter work profile) for less tracking.

Rule: Replace what you can, keep what you must. Level 1 is about adding choice, not creating hardship.

LEVEL 1 • STILL ZERO RISK

Aurora Store — Play Store Without Google

- Install Aurora Store from F-Droid, open it, tap Anonymous — no Google login needed.
- Install BHIM, IRCTC, UMANG, WhatsApp through Aurora, Google-account-free.
- Prefer BHIM (NPCI) for UPI — it's built for this, unlike GPay and other bank-linked apps.
- Play Services stays installed at this level — banking/UPI apps work exactly as before.
- In Aurora Settings, note “Filter Google Play Services dependent apps” — useful later, if you ever reach Level 3.

Same apps. No account.

Aurora Store is still Level 1 — nothing is removed, nothing is at risk. It's simply a second front door into the same Play Store catalog, one that doesn't ask Google who you are.

SMALL WIN, REAL PROGRESS

Take a Breath.

You Just Did Level 1.

No root. No data loss. Nothing to undo.
That's not a demo — that's done.

Level 2 is next, if you want it. There's no rush.



LEVEL 2

Break the Dependency

~1 hour · Needs some confidence

- Remove pre-installed Google apps via ADB — no root needed.
- MicroG replaces Play Services for push notifications, if you remove it.
- Builds on Level 1 — Aurora Store already has Play Store apps covered.
- Reversible: apps are disabled per-user, not wiped from the device.

LEVEL 2 · IF YOU REMOVE PLAY SERVICES

MicroG for Notifications

- MicroG is a Free Software reimplementation of Google Play Services.
- It only matters if you fully remove Play Services — if you kept it, skip MicroG entirely.
- Some apps (banks, delivery) need Google Cloud Messaging for push notifications — MicroG replaces that.
- Install via F-Droid (add the MicroG repo), or just use /e/OS or CalyxOS at Level 3, which ship with it built in.

Indian Reality Check

Most Indian banking/UPI apps fail SafetyNet if Play Services is removed — BHIM is the most likely to keep working. Test yours before removing fully; keep Play Services if you depend on GPay or another bank app for business.

LEVEL 2 · FOR WHEN YOU'RE READY

Degooglify
your phone by
removing
these apps!



Degooglify
verb

- To get rid of all services and applications of a device that are created/ hosted by the Google company.

Google applications tracks and stores our data. To prevent this, Degooglifying is necessary.



adb devices

adb shell

(Enable Android Debugger by touching the build number multiple times)

Run **pm uninstall -k --user 0**

<package_name> to remove the app from your device.

The package names of various Google apps are listed below:

	Maps	com.google.android.apps.maps
	Photos	com.google.android.apps.photos
	Docs	com.google.android.apps.docs
	Duo	com.google.android.apps.tachyon
	Chrome	com.android.chrome
	YouTube	com.google.android.youtube
	Play Music	com.google.android.music
	Play Videos	com.google.android.videos
	Play games	com.google.android.play.games
	Play books	com.google.android.apps.books

 / Free Software Movement of India

 fsmi.social/fsmi



LEVEL 3

Liberate

For enthusiasts & community phones

- Install a custom ROM: LineageOS, /e/OS, GrapheneOS, or CalyxOS.
- Full de-googling — no Google code left on the device, if you choose.
- Best for enthusiasts, older phones, or shared/community devices.
- Be honest: voids warranty, and banking apps needing SafetyNet may not work.

LEVEL 3 · WHICH ROM FOR INDIA

Choosing Your ROM

LineageOS

No Play Services (MicroG optional)

Largest device support — Redmi Note, POCO, OnePlus, Motorola, older Samsungs. Best for students & tinkerers.

/e/OS (Murena)

MicroG built-in — apps just work

The 'it just works' degoogled ROM. Best for non-technical people, activists, NGOs, workshop demo phones.

GrapheneOS

Sandboxed Play Services (optional)

Google Pixel only (6/7/8). Security-hardened, gold standard — but not for the average Indian phone.

CalyxOS

MicroG built-in

Pixel + some Xiaomi. Built-in firewall + free VPN. Balanced privacy and ease of use.

For India, start with LineageOS + MicroG, or /e/OS.

Before You Flash

- Check your phone is supported:
wiki.lineageos.org/devices or doc.e.foundation/devices.
- Unlocking the bootloader wipes all data — backup photos, WhatsApp, note your UPI PIN.
- Xiaomi: 7-day wait via Mi Unlock Tool. OnePlus: instant. Samsung Snapdragon: hard.
- Realme/OPPO/Vivo are often NOT unlockable in India — check before you buy, not after.
- Keep a second phone handy for OTPs on flashing day.

THE FOUR STEPS

1. Unlock the bootloader.
2. Flash custom recovery (TWRP / Lineage Recovery).
3. Factory reset, then sideload the ROM zip.
4. Reboot — first boot takes 10–15 minutes.

LEVEL 3 · INDIAN APP SURVIVAL KIT

Life After Flashing

UPI / BHIM

Via Aurora Store (Anonymous). BHIM works with MicroG — prefer it over GPay and other UPI apps.

WhatsApp

Via Aurora Store. Restore local backup, disable Google Drive backup.

UMANG / IRCTC

Via Aurora Store — works fine with MicroG.

Maps for delivery/taxi work

Organic Maps offline, or GMaps via Aurora inside a Shelter work profile.

YouTube

NewPipe or LibreTube — no Google account needed at all.

Should you do Level 3? Yes — even if it's your only phone, a spare device, a community library phone, or you just love tinkering. No — if you depend on GPay for income or you need warranty. Stay at Level 1/2 if either applies — that's already huge.

MIDPOINT CHECK-IN

That Was the Hard Part.

Three levels. Real technical depth — more than most phone owners ever bother to touch.

What's left is easier: the practical questions everyone asks, and what you actually gain from all this.

FAQ: Money & Apps You Depend On

Q: Will UPI (GPay/PhonePe/BHIM) stop working?

No, at Level 1 or 2 with Play Services kept. At Level 3, BHIM/PhonePe work with MicroG; GPay sometimes fails SafetyNet. Keep BHIM as your primary UPI on a degoogled phone.

Q: Will I lose my WhatsApp chats?

No. Switch backup to local storage before you start: WhatsApp → Settings → Chats → Chat Backup → Back up to local storage. Your chats stay on the phone either way.

Q: Can I still use IRCTC, UMANG?

Yes — install via Aurora Store (Anonymous mode) after Level 2. Most work fine with MicroG; use Shelter to isolate anything that doesn't.

FAQ: Risk & Reality

Q: Will my banking app detect root or a custom ROM and block me?

Not at Level 1 or 2 — no root involved. At Level 3, some apps (SBI YONO, HDFC, ICICI) check SafetyNet and may block. If banking is critical on your only phone, stay at Level 2.

Q: Is this legal? Will it void my warranty?

Levels 1 & 2 are fully legal, warranty intact. Level 3 (unlocking) is legal — you own the device — but may void manufacturer warranty as company policy, not law.

Q: My phone is Realme/Vivo/OPPO — can I do Level 3?

Likely no — BBK Group locks bootloaders in India. Level 1 & 2 still work fully. Next purchase, look at Motorola, Nothing, OnePlus, or Pixel for unlock-friendly options.

FAQ: Why This, Why Us

Q: What about data? Will I still need Google?

No. F-Droid apps need far less data. Organic Maps offline saves huge amounts on maps. NewPipe's ad-blocking alone saves ~30% of YouTube data — students report 500MB–1GB/month saved.

Q: I need Google Classroom/Docs/Drive for college?

Keep them at Level 1. From Level 2 on, use Firefox instead of the app — classroom.google.com works fine in-browser, with less tracking and no background permissions.

Q: Who's behind this?

FSMI is an Indian non-profit coalition since the 2000s. This is a pro-India digital sovereignty campaign — CCI itself found Google abused its dominance. We're on the same side as Indian law.

PERFORMANCE, LEVEL BY LEVEL

Will This Make My Phone Faster?

Yes — less background competition for RAM and CPU means snappier everything, at every level.

1

Level 1: Modest but real

Lighter FOSS apps (Firefox, NewPipe, Organic Maps) launch faster and use less RAM than their bloated Google counterparts — no dramatic change, but every swap helps.

2

Level 2: The real jump

Removing 20–40 pre-installed background apps frees up RAM and CPU cycles that were fighting your foreground app for resources. Users report noticeably faster app launches after Level 2 de-bloat.

3

Level 3: Feels like a new phone

A lean custom ROM with no OEM skin or bloat boots faster and stays consistently smooth — LineageOS on old hardware routinely feels faster than the day you bought it.

BATTERY, LEVEL BY LEVEL

What About Battery Life?

Every background wake-up costs battery. Fewer background processes, more hours on a charge.

1

Level 1: Fewer wake-locks

FOSS replacements don't phone home in the background the way their Google counterparts do — fewer trackers and analytics calls means fewer battery-draining wake-ups. Modest, but adds up over a day.

2

Level 2: 15–25% gains, reported

Removing pre-installed background apps is the single biggest lever on a budget phone. Users report 15–25% battery gains after Level 2 de-bloat — this is where the real difference shows up.

3

Level 3: The drain is gone

Google Play Services — the #1 background battery drain on Indian budget phones — is stripped out entirely on a custom ROM. Old hardware routinely goes a full extra day on the same battery.

ANOTHER REASON THIS IS WORTH IT

Data Saved = Money Saved

The average Indian netizen uses ~1.04 GB of mobile data a day (Nokia MBiT Index, 2026) — here's what you keep back.

YouTube via NewPipe	50–150 MB/day	Each skipped video ad costs ~3–5 MB at typical mobile quality. For 10–20 videos watched a day, that's the single biggest line on this slide — more for heavy watchers.
Browsing via Firefox + uBlock Origin	~40%	Blocks ads and trackers before they load — biggest savings on news and content-heavy sites.
Maps via Organic Maps (offline)	~100%	Download your district once, then navigate with zero data — no streaming map tiles.
Photo/video backup, local or Wi-Fi-only	GBs/mo	Google Photos auto-uploads originals over mobile data by default — the single biggest hidden drain for camera-heavy users.
Background telemetry blocked (NetGuard/TrackerControl)	ongoing	Every app idling in the background still phones home — blocking it stops the constant small pings that add up all day.

~60–200 MB

saved every day — mostly video ads (2–6 GB/month)

Data isn't free. Every megabyte you don't spend on ads and trackers is money you don't spend on your next recharge.

NO MORE WAITING

Time Saved = Time Back

Every skipped ad and faster page load is a second you get back — they add up fast.

Browsing via Firefox + uBlock Origin **~30% faster**

Pages render without waiting on ad and tracker scripts to load first — up to 38% faster on mobile, per independent ad-blocker benchmarks.

YouTube via NewPipe **0 sec of ads**

No 15–30 second forced pre-roll ads before every video, no waiting to tap 'Skip Ad' — the video just starts.

De-bloated phone (Level 2) **less lag**

Fewer background apps competing for RAM and CPU means faster app switches and fewer 'phone is thinking' freezes.

Custom ROM (Level 3) **faster boot**

A lean ROM boots faster and skips the OEM startup animations, setup nags, and bundled-app first-run screens.

Meanwhile, Google is adding a wait, not removing one.

From Sep 2026, Google's own 'advanced flow' for sideloading demands a mandatory 24-hour wait and 9 steps — just to install an app you already chose. The time FOSS gives back, Google's new policy takes away.

THE ORIGINAL REASON, QUANTIFIED

Privacy Gains, Level by Level

Speed, battery, data, and time were the side effects. This is the actual point.

1

Level 1: Stop the visible leaks

Pause and delete Location History, Web & App Activity, YouTube History, Ad Personalization — the exact tracking you saw on myactivity.google.com earlier, switched off.

2

Level 2: Remove the trackers themselves

Uninstalling Google's apps removes their embedded SDKs — Firebase Analytics, AdMob, Crashlytics — the same trackers found in a majority of all scanned Android apps, gone from your device.

3

Level 3: No channel left to leak through

Google Play Services — the backbone that makes background tracking possible at all — is gone entirely. Nothing left to phone home, even for apps that would try.

PART TWO

You Now Know How.

Here's why it matters.

Three levels. Real gains — speed, battery, data, time, privacy. None of it was a sacrifice.

Now the harder question: why does the easy path always seem to be the one that watches you?

That's not an accident. That's design.

“

Google isn't afraid of critics.

**It's afraid of Android users who've tasted freedom —
because once you know your phone is malleable
and can be made better, there's no going back.**

That fear is why it restricts. That fear is why it discourages.

That fear is why every desperate measure keeps arriving, one policy at a time.

— FSMI, #DeooglefyAndroid

DARK PATTERNS EXPLAINED

The Tricks That Keep You Locked In

Dark patterns: design tricks that steer you away from the choice you'd actually make.

Confirmshaming

"Skip protecting my data" — framed as the wrong answer.

Pre-checked by default

Location & ad personalization: on by default, buried in settings.

Friction asymmetry

One tap to enable a service, five taps + scare screens to disable it.

Roach motel

Easy to sign in, hard to fully delete your account data.

Nagging

Repeated prompts to re-enable Assistant, backup, location after you say no.

Sound familiar? The 9-step “advanced flow” to sideload apps after Sep 2026 is friction asymmetry at Android-OS scale.

Confirmshaming

WHAT IT IS

Wording the option you'd actually pick as if it's the wrong, careless, or shameful choice.

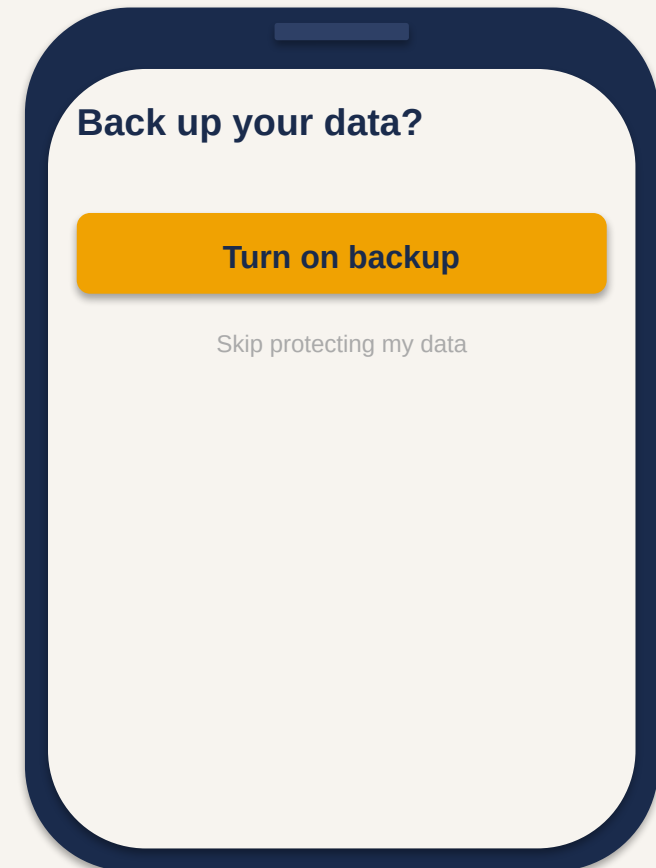
GOOGLE'S VERSION

During setup and permission prompts, declining tracking is worded like a risk: “Skip protecting my data”, “No thanks, I don't want a faster phone.” The button that keeps your data private sounds like the one that leaves you exposed.

WHY IT WORKS

Nobody wants to tap something that sounds irresponsible — even when it's the privacy-respecting choice. The guilt does the persuading, not the actual tradeoff.

EXAMPLE SCREEN



Pre-Checked by Default

WHAT IT IS

The option that shares more data is switched ON before you ever touch the screen — opting out takes effort, opting in takes none.

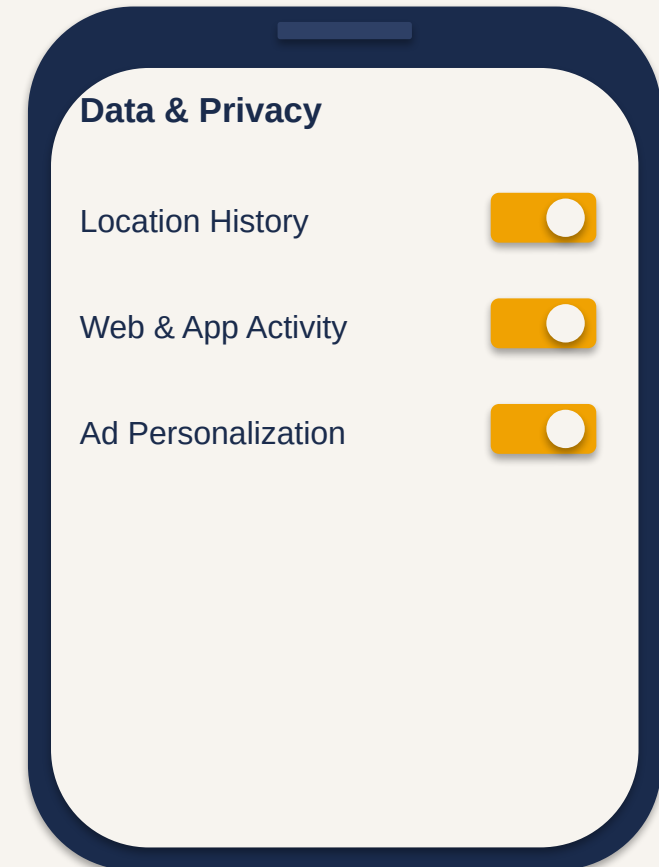
GOOGLE'S VERSION

Location History, Web & App Activity, YouTube History, and Ad Personalization all ship enabled during phone setup. Turning them off means finding Settings → Google → Data & Privacy — a path most people never take.

WHY IT WORKS

Most users never change a default (“default bias”). Pre-checking one box is the same as opting nearly every user in, at scale, without asking anyone directly.

EXAMPLE SCREEN



Friction Asymmetry

WHAT IT IS

Turning a feature on takes one tap. Turning the same feature off takes many, on purpose.

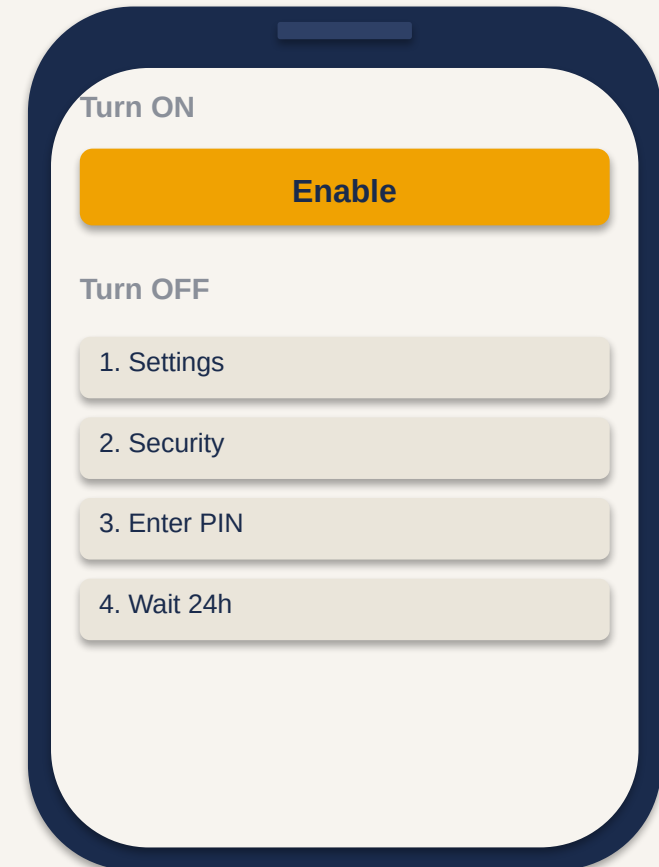
GOOGLE'S VERSION

Enabling Assistant, Location, or backup is instant. Disabling deep-linked Google services often means hunting through nested menus, re-confirming choices, and dismissing repeated warnings.

WHY IT WORKS

Friction is a tax on the choice Google doesn't want you to make. Most people don't abandon the decision — they just give up partway through the flow.

EXAMPLE SCREEN



Roach Motel

WHAT IT IS

Easy to check in, deliberately hard to check out — named for the old ad line: roaches check in, but they don't check out.

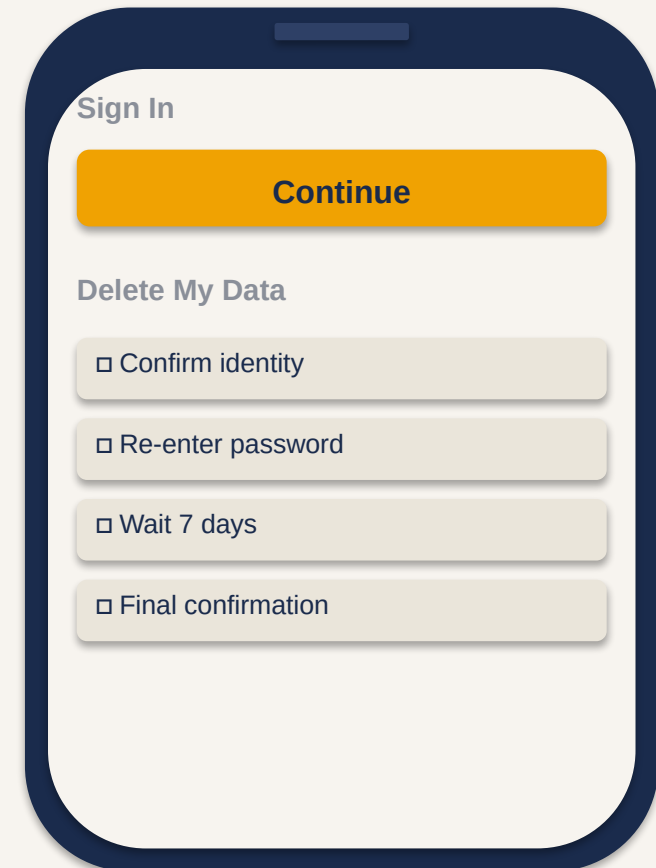
GOOGLE'S VERSION

Signing into a Google Account takes seconds. Fully deleting your data — activity history, ad profile, stored files — means navigating multiple settings screens, confirmations, and waiting periods, and some of it persists elsewhere regardless.

WHY IT WORKS

Exit costs — time, uncertainty, fear of losing something — keep people locked in long after they've already decided to leave.

EXAMPLE SCREEN



Nagging

WHAT IT IS

A declined choice isn't final — the same prompt reappears until fatigue wins.

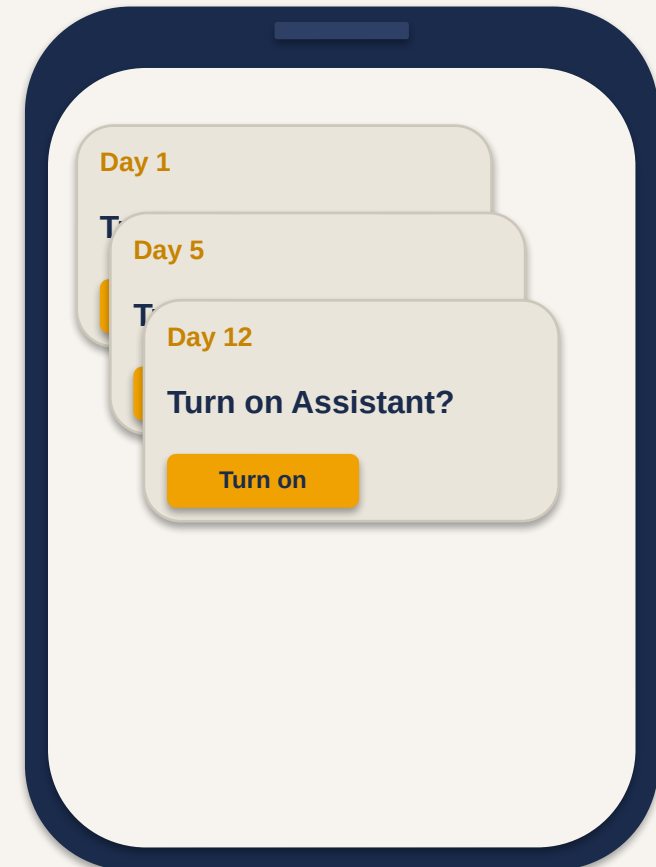
GOOGLE'S VERSION

Say no to Assistant, backup, or location once, and the prompt returns after the next app update, restart, or feature rollout — worded slightly differently each time, as if you hadn't already answered.

WHY IT WORKS

Every 'no' is treated as temporary. Every 'yes' is treated as permanent. Eventually, saying yes for the tenth time is easier than saying no again.

EXAMPLE SCREEN



SOUND FAMILIAR?



Every dark pattern on the last slide, in one panel.

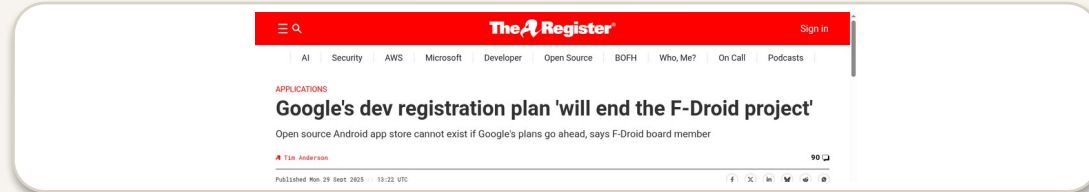
Sideloading & App Stores: Google's Policy Timeline



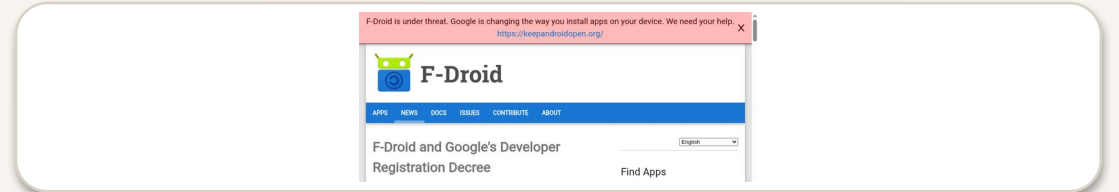
THIS IS BEING COVERED, NOT JUST DEBATED

In the Headlines: The Global Fight

Real coverage of the events on the last slide — screenshots captured directly from each outlet.



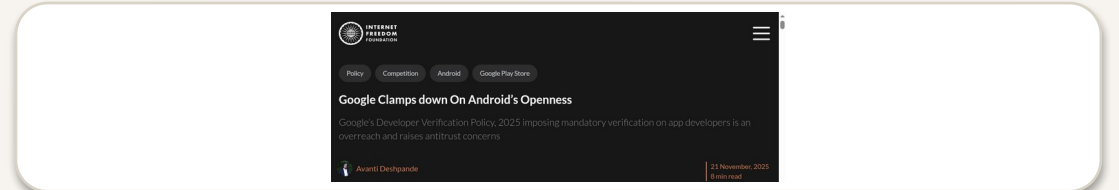
The Register (Sep 29, 2025)



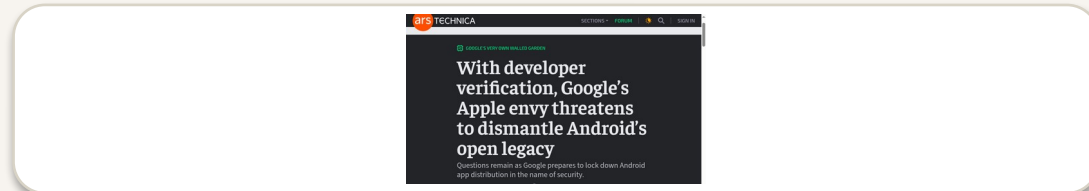
F-Droid Official Blog (Sep 29, 2025)



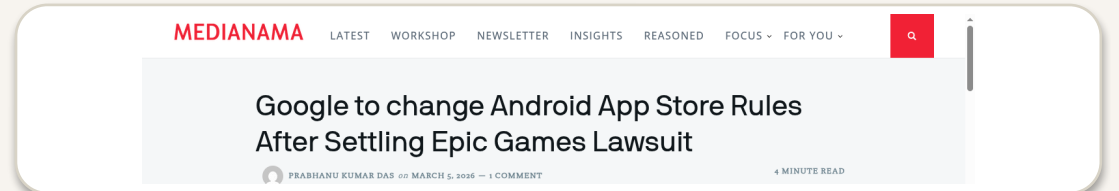
Android Headlines (Oct 29, 2025)



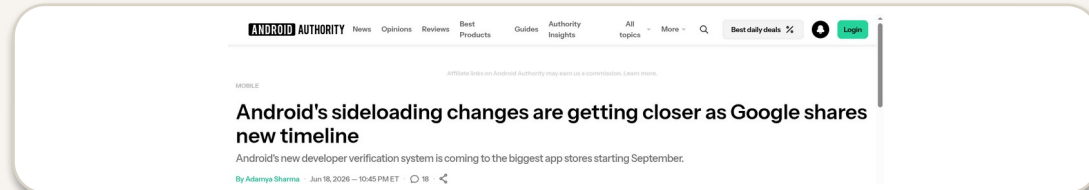
Internet Freedom Foundation (Nov 21, 2025)



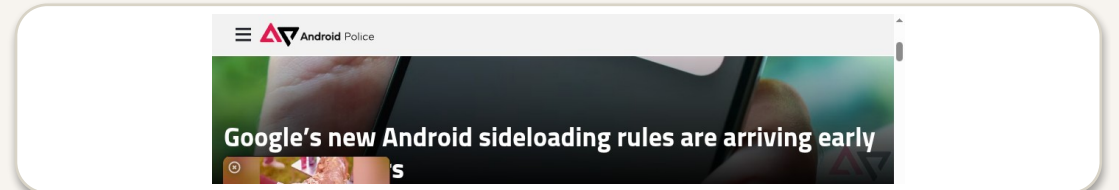
Ars Technica (Mar 3, 2026)



MediaNama (Mar 5, 2026)



Android Authority (Jun 18, 2026)



Android Police (Aug 19, 2026)

September 2026: The Real Deadline

- Google now requires developer ID verification.
- Unverified apps get blocked on Android.
- Sideloading, F-Droid — also affected.
- This is about your future choice, not just privacy.



IN CASE THE LAST SLIDE DIDN'T LAND



Your phone. Your money. Your choice — not Google's permission slip.

FOUR CLAIMS, FOUR CHECKS

Is This Really About Security?

Google has given four justifications for Developer Verification. Let's check each one against the public record.

1. "Sideloaded apps have 50x more malware."
2. "This only affects an advanced power-user flow."
3. "Verification isn't Play Store review — sideloading still works."
4. "This is purely a security measure."

“Sideloaded apps have 50x more malware than Play Store apps.”

THE RECORD SHOWS

- Google's own blog: “over 50 times more malware from internet-sideloaded sources.”
- F-Droid's official response (Oct 2025): “We haven't seen this recent analysis — or any other supporting evidence.”
- No published methodology means no one can verify, replicate, or challenge the number.
- A claim this consequential, used to justify gating billions of devices, needs evidence that can survive scrutiny.

An unpublished study can't be checked — and can't be trusted to justify a global policy change.

“This only affects an advanced power-user flow.”

THE RECORD SHOWS

- The average user was never sideloading — this claim quietly shifts who's really affected.
- Real impact: college-project apps, community health apps, anonymous privacy tools, NGO-built apps.
- Anonymous or sanctioned-region developers can't complete ID verification at all — exclusion by birthplace.
- F-Droid — an entire alternate app ecosystem, not an edge case — is exactly what gets gated.

The people actually blocked are students, NGOs, and activists — not power users.

“Verification isn't Play Store review — sideloading still works.”

THE RECORD SHOWS

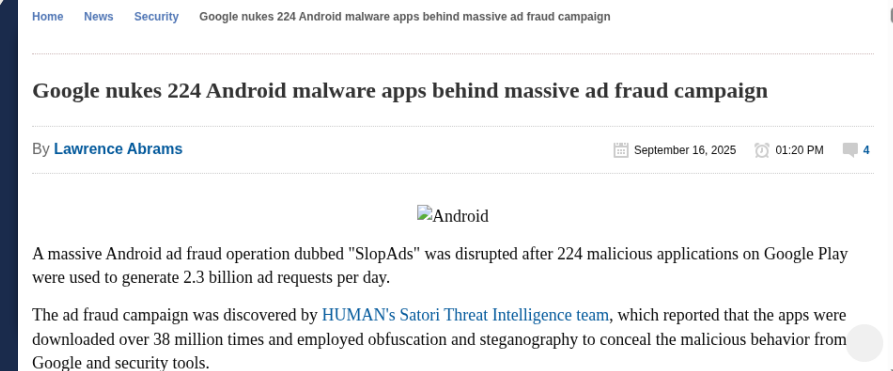
- The 'advanced flow': tap build number 7×, dismiss scare screens, enter a PIN, restart, wait 24 hours.
- Then: dismiss more scare screens, choose “allow 7 days” or “allow indefinitely,” confirm again.
- This runs through Play Services, not the OS — Google can revoke or tighten it silently, no OS update needed.
- F-Droid and EFF both call this a deterrence mechanism, not a real permission.

**Nine steps. A 24-hour wait.
Delivered through Play
Services — which Google can
tighten, or kill, at any time.**

“This is purely a security measure.”

THE RECORD SHOWS

- Google Play Protect already scans sideloaded apps for malware — independent of developer ID.
- CCI (2022) and a US court (Epic v. Google, Oct 2024) both already found Google abused Android market dominance.
- If security were the only goal, scanning — which already exists — solves it.
- ID + fee + signing-key evidence solves a different problem: who's allowed to distribute software at all.



BleepingComputer, Sep 16, 2025 — “Google nukes 224 Android malware apps behind massive ad fraud campaign”
224 malicious apps. 38 million downloads.
Removed from Google's own store — in 2025, the same year they announced this.

WHO ACTUALLY DEFENDS YOU?

FOSS Communities: The Watchdogs of Digital Rights

- Exodus Privacy — scans any app's APK for trackers, publishes every report free.
- Let's Encrypt — made HTTPS free, encrypting most of the web almost overnight.
- EFF, FSF & FSMI — decades of digital-rights litigation, advocacy, and campaigning, volunteer-funded.
- F-Droid — the reason a Google-free app store is even possible today.

Not one of them is a company.

Volunteers, non-profits, hacktivist collectives — not the corporations being audited. That's not a coincidence: a watchdog can't be owned by what it watches.

Exodus isn't the exception. It's the pattern.

FOSS communities have been on the right side of digital-rights history, again and again.

THE DATA, NOT JUST THE DEMO

Side by Side: Trackers & Permissions

Permission counts are manifest facts. Tracker counts are a methodology, not a clean bill of health — see note below.

YouTube

25+ permissions (partial) · trackers: unconfirmed

Google Maps

34 permissions · trackers: unconfirmed

Gmail

66 permissions · trackers: unconfirmed

Google Keyboard

16 permissions · trackers: unconfirmed

Play Store

permissions & trackers: unconfirmed

NewPipe

0 trackers · 12 permissions

Organic Maps

0 trackers · 26 permissions

Thunderbird / K-9 Mail

0 trackers · 10 permissions

FlorisBoard

0 trackers · 3 permissions

Aurora Store

24 permissions · shares app list w/ Google by default

Exodus's static analysis matches KNOWN third-party SDK signatures — it's not built to catch Google's own first-party telemetry inside Google's own apps. "Trackers: unconfirmed" means exactly that, not "zero." Aurora Store itself isn't spotless either: it sends your app list to Google's servers by default (F-Droid Tracking anti-feature).

CCI vs Google: Timeline of Enforcement



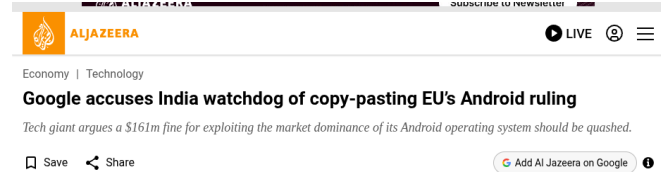
THIS IS BEING COVERED, NOT JUST DEBATED

In the Headlines: The CCI Case

Real coverage of the events on the last slide — screenshots captured directly from each outlet.



CCI Official Press Release (Oct 20, 2022)



Al Jazeera (Jan 4, 2023)



TechCrunch (Jan 19, 2023)



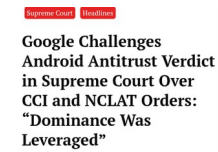
Bar & Bench (2023)



Business Standard (Mar 29, 2023)



Outlook Business (Mar 29, 2025)



LawChakra (Jul 24, 2025)

GLOBAL + INDIA

The Keep Android Open Campaign

Same fight, two fronts — sign globally, act locally.



GLOBAL

keepandroidopen.org

- 71+ orgs signed: EFF, F-Droid, LineageOS, GrapheneOS, FSF.
- Open letter + Change.org petition — 100k+ signatures.
- Demand: reverse mandatory developer ID verification.



INDIA

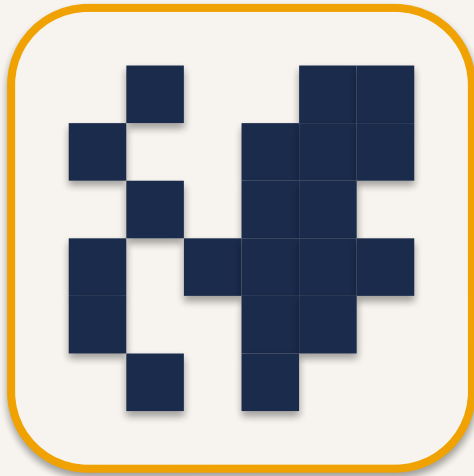
keepandroidopen.in

- Co-initiated by FSFTN, FSHM, FSMK, Swecha Telangana, Swecha AP.
- One-tap email straight to the Competition Commission of India.
- Asks CCI to rule ID-gated sideloading an abuse of dominance.

DO IT NOW

Three QR Codes, Right Now

- Scan one: install F-Droid. Scan two: add the FSMI repo. Scan three: email the CCI.
- Takes under three minutes, all three. Phones out — let's do it together.



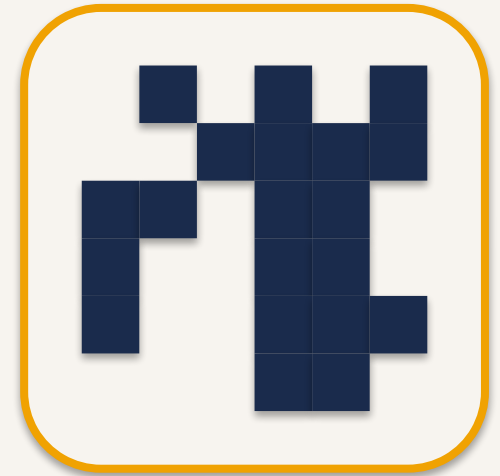
F-Droid

f-droid.org



FSMI Repo

apps.fsmi.in/fdroid/repo



Keep Android Open

keepandroidopen.in

BEYOND TODAY

Join This Campaign

WAYS TO GET INVOLVED



Organise Install Fests

Run hands-on Level 1 sessions in your college, LUG, or community centre.



Local-Language Social Campaigns

Carry #DegooglefyAndroid in Tamil, Telugu, Malayalam, Kannada, Bengali & beyond.



Localise Guides & Material

Translate GUIDE-Beginner, GUIDE-Advanced, and the FAQ into your state language.



Make Campaign Material

Posters, short videos, memes — help the message travel further than we can alone.

BEYOND TODAY

Contribute to FreeTheAndroid Initiative

THREE PROJECTS, ONE PER LEVEL — PICK WHERE YOU CAN HELP

LEVEL 1

FSMI F-Droid Repo

Encourage FSMI member orgs to build & publish more FOSS apps.

Help member organisations package their FOSS apps and get them published to F-Droid.

LEVEL 2

Android De-bloater TUI app

A terminal UI on top of ADB — de-bloating with no command line.

Help build the tool that makes Level 2 accessible to non-developers.

LEVEL 3

Custom ROM Builder

Help build & maintain an FSMI-flavoured degoogled ROM.

Device testing, build maintenance, and documentation for Indian phone models.

THANK YOU

- You just reclaimed part of your phone.
- Write your experience of switching to mobile freedom, tag us.
- Help your friends and Family to break out from chain of Google and switch to the side of Mobile Freedom.
- FSMI: fsmi.in

#DegooglefyAndroid

Ranjith Raj · ranjithraj@fsmi.in · +91 9533589259