

Die Schließung von Android: Wie ein auf freien Beiträgen errichtetes Betriebssystem gegen seine eigenen Nutzer versiegelt wird

Geboren aus der Allmende – und ein frühes Warnsignal

Android entstand nicht in einem Labor von Google. Es entstand, in einem sehr realen Sinne, Jahrzehnte früher – in den Mailinglisten, Code-Repositories und freiwilligen Arbeitsstunden der Freie-Software-Bewegung.

Als Android Inc. im Jahr 2003 von Andy Rubin und drei Kollegen gegründet wurde, war es ein Start-up mit weniger als einem Dutzend Mitarbeitern. Was ein Betriebssystem für ein so kleines Team überhaupt erst möglich machte, war nicht Genialität allein, sondern ein gewaltiges Erbe: der **Linux-Kernel**, damals bereits mehr als ein Jahrzehnt gereift und das Ergebnis von Tausenden Personenjahren Arbeit; **SQLite** für die Datenspeicherung; **WebKit** für die Darstellung des Webs; **FreeType**, **OpenSSL**, die GNU-Werkzeugkette und Dutzende weiterer Komponenten. Die Menschen, die dieses Fundament errichteten, mussten keine Gebühren zahlen, sich nirgends registrieren und keine Identitätsnachweise erbringen. Für das Mainstream-Linux gilt das bis heute: Beitrag und Nutzung werden durch Qualität und Lizenzbedingungen geregelt, nicht durch Identitätspreisgabe oder Zahlungen an einen Konzern-Türwächter. Google übernahm Android 2005 für geschätzte 50 Millionen Dollar, lieferte 2008 das erste Gerät aus – und heute läuft das System auf mehr als drei Milliarden Geräten, jedes einzelne mit der unbezahlten und unregistrierten Arbeit der Freie-Software-Gemeinschaft in seinem Kern.

Doch wer verstehen will, wohin sich dieses Ökosystem entwickelt, sollte ein oft übersehenes Kapitel kennen: **Bereits 2018/2019 zeigte Google, wie es mit unabhängigen Dienstleistern umzugehen gedenkt.** Am 31. August 2018 kündigte David Graff, Googles Direktor für weltweite Produktpolitik, eine globale Werberichtlinie an, die ab dem Frühjahr 2019 – im deutschsprachigen Raum spürbar ab April/Mai 2019 – **unabhängigen Reparaturbetrieben und Drittanbietern von technischem Support pauschal den Zugang zu Google-Werbeanzeigen sperrte.** Die Begründung: irreführende Werbeerfahrungen einzelner schwarzer Schafe. Die Wirkung: Seriöse, teils langjährige Werbekunden verloren über Nacht ihre Sichtbarkeit im dominierenden Werbekanal des Internets – ohne Vorwarnung, ohne klare Freischaltungsbedingungen, ohne zuständigen und entscheidungsbefugten Ansprechpartner. Das für die Folgemonate angekündigte Verifikationsverfahren, mit dem sich seriöse Anbieter hätten freischalten lassen können, wurde nie regulär eingeführt; im September 2019 verkündete Google stattdessen, die Sperre auf unbestimmte Zeit fortzusetzen. Zugleich zeigten sich bezeichnende Asymmetrien: Große Handelsketten warben weiter unbeanstandet für Smartphone-Reparaturen, und wer eine gut vernetzte Werbeagentur mit Kontakten zu Google beschäftigte, konnte manuelle Wiederfreischaltungen noch am selben Tag erwirken – während kleine Betriebe ohne solche Kanäle messbare wirtschaftliche Schäden erlitten und

sich an Wettbewerbszentrale, Bundeskartellamt und EU-Kommission wandten. Dass Google zu diesem Zeitpunkt selbst einen eigenen Reparaturdienst aufbaute und wirtschaftlich eng mit Apple verflochten war – einem Hersteller, der unabhängige Reparaturen seiner Geräte juristisch bekämpfte – warf zusätzlich die Frage nach einem Interessenkonflikt auf. Ein Betroffener zitierte damals eine Auskunft des Google-Supports, wonach „Interessenkonflikte zwischen Herstellern und Drittanbietern“ bestünden, die es zu lösen gelte.

Das Muster, das sich hier zum ersten Mal in voller Klarheit zeigte, wird den Leser durch diesen gesamten Artikel begleiten: **Ein reales Missbrauchsproblem dient als Begründung für eine pauschale, weltweite Sperre; das versprochene faire Prüfverfahren bleibt aus oder undurchsichtig; die Last trägt der kleine, unabhängige Akteur; und der Gatekeeper, der über Zugang und Ausschluss entscheidet, verfolgt im selben Markt eigene kommerzielle Interessen.** Was 2019 die unabhängigen Reparaturbetriebe traf – also genau jene, die Gerätelebensdauern verlängern und Elektroschrott vermeiden –, trifft ab 2026 die unabhängigen Softwareentwickler. Es ist dieselbe Schlagrichtung, nur eine Ebene tiefer: erst die Sichtbarkeit der Reparatere, jetzt die Software selbst - beides unterhalb der Gürtellinie.

Was Offenheit dem Nutzer gab

Die Offenheit von Androids Ursprüngen war nie bloß eine Bequemlichkeit für Entwickler. Sie übersetzte sich unmittelbar in **Nutzerfreiheiten**:

- **Das Recht, beliebige Software auszuführen.** Jeder Nutzer konnte per Schalter in den Einstellungen jede Anwendung installieren – von einem Freund, einer Webseite, einem Community-Repository wie F-Droid – ohne die Genehmigung irgendeines Konzerns.
- **Das Recht auf ein zweites Leben für Hardware.** Wenn Hersteller ihre Geräte nach zwei oder drei Jahren aufgaben, sprangen Gemeinschaften wie LineageOS ein und lieferten aktuelle, sichere Betriebssysteme für Telefone, die die Industrie bereits abgeschrieben hatte. Millionen Geräte gewannen Jahre zusätzlicher Nutzungsdauer.
- **Das Recht auf Ausstieg.** Ein Nutzer konnte, mit etwas Aufwand, ein entgoogeltes Android betreiben – ohne Tracking, ohne Zwangsdienste – und dennoch ein funktionierendes Smartphone besitzen.
- **Das Recht auf lokale Software im Kleinen.** Ein Student konnte eine App für ein Seminarprojekt bauen. Eine Kirchengemeinde konnte eine Termin-App an ihre Mitglieder verteilen. Ein gemeinnütziger Verein konnte Freiwilligen ein maßgeschneidertes Erfassungswerkzeug in die Hand geben. Nichts davon erforderte Gebühren, Prüfverfahren oder Registrierung.
- **Reparieren, umnutzen, spenden.** Alte Telefone wurden zu Überwachungskameras, Medien-Fernbedienungen, Sensorzentralen und Spendengeräten für Menschen, die sich keine neuen leisten konnten – fast immer mittels frei installierter Software.

Das war der stillschweigende Vertrag von Android: Aus der Allmende gebaut, blieb es – zumindest teilweise – eine Allmende für seine Nutzer.

Die sukzessive Einhegung

Genauso wie die Letter des Mottos „Don't be evil“ an den Wänden des Googleplex Gebäudes, wurde dieser Vertrag inzwischen demontiert, jede einzelne Etappe davon zum wirtschaftlichen Vorteil der Firma:

1. **Die Dienste-Abwanderung (ab 2012).** Google verlagerte Funktionalität schrittweise aus dem offenen AOSP in die proprietären Google Play Services. Der „offene“ Kern wurde von Jahr zu Jahr hohler; immer mehr Apps funktionierten ohne Googles geschlossene Schicht nicht mehr.
2. **Vertragliche Kontrolle der Hersteller.** Der Zugang zum Play Store und zu Google-Apps erforderte Vereinbarungen, die die Hersteller an Googles Bedingungen banden – vorinstallierte Apps, Platzierungsvorgaben, Anti-Fragmentierungs-Klauseln.
3. **Die Aussperrung der unabhängigen Reparatere (2018/2019).** Wie eingangs geschildert, sperrte Google Drittanbieter von Reparatur- und Supportdienstleistungen weltweit von seiner Werbepattform aus – mit Sicherheitsbegründung, ohne funktionierendes Freischaltungsverfahren und mit spürbarer Schonung großer, umsatzstarker Akteure.
4. **Das Anziehen der Zügel im Store.** Gebühren, Prüfrichtlinien, Testanforderungen und Identitätsverifikation für die Play-Store-Veröffentlichung hoben die Hürde für kleine Entwickler stetig an.
5. **Die letzte Tür (angekündigt im August 2025, wirksam ab September 2026).** Unter Googles neuem Verifikationsregime muss sich **jeder Entwickler bei Google registrieren** – eine Gebühr zahlen, Googles Bedingungen zustimmen, einen amtlichen Ausweis vorlegen und seine Anwendungskennungen deklarieren – bevor seine Apps auf zertifizierten Android-Geräten installiert werden können. Nicht nur Play-Store-Apps: auch seitlich installierte Apps, F-Droid-Apps, Apps, die unter Freunden geteilt werden. Nicht registrierte Software wird auf Geräteebene blockiert.

Man beachte die Eleganz des Manövers: Google musste den Quellcode nie schließen. AOSP bleibt nominell offen. Aber die Offenheit des *Codes* bedeutet wenig, wenn die *Geräte* – die zertifizierten Telefone in den Taschen von Milliarden Nutzern – sich weigern, Software auszuführen, deren Urheber sich nicht bei einem einzigen amerikanischen Konzern registriert, bezahlt und ausgewiesen hat. Die Allmende wurde nicht geschlossen; sie wurde unerreichbar gemacht.

Und all das von einem Unternehmen, das bereits auf jeder Ebene an Android verdient: Umsatzbeteiligung an App-Verkäufen und In-App-Käufen (Milliarden jährlich), Hardware-Verkäufe, Zahlungen für Suchmaschinen-Voreinstellungen, Werbung – und vor allem die fortlaufende Extraktion von Nutzerdaten auf der weltweit dominierenden Mobilplattform. Ergo, das Verifikationsregime ist keine finanzielle Notwendigkeit: Es ist ein Gesslerhut

ersten Ranges, gerechtfertigt mit dem Gemeinplatz der Sicherheit, dessen Kosten fast vollständig auf jene abgewälzt werden, die sie am wenigsten tragen können.

Wer zahlt – die implizit Getroffenen

Die Last dieser Politik ist mit bemerkenswerter Präzision verteilt. **Große kommerzielle Entwickler zahlen praktisch nichts** – sie verfügen bereits über Rechtsabteilungen, Handelsregistereinträge und verifizierte Konten. Die Kosten treffen:

- **Hobbyisten und Studierende**, für die eine Gebühr, juristische Vertragsbedingungen und die Preisgabe der Identität für eine einzige private App ein Ausschlusskriterium sind. Ein Großteil dieser Software wird schlicht nie geschrieben werden.
- **Gemeinnützige Organisationen, Gruppen und Ehrenamtliche**, deren interne Werkzeuge und Apps für kleine Zielgruppen keinen laufenden Compliance-Aufwand rechtfertigen können.
- **Open-Source-Entwickler**, von denen viele die Identitätsregistrierung bei einem Konzern aus Prinzip ablehnen – das exakte Gegenteil der Kultur des anonymen Beitrags, auf der Androids eigenes Fundament errichtet wurde.
- **Entwickler unter repressiven Regimen**, für die Anonymität keine Ideologie ist, sondern Sicherheit. Ein Dissident, der eine Zensurumgehungs- oder Schutz-App verbreitet, kann keinem US-Konzern, der behördlichen Herausgabeverlangen unterliegt, seinen Ausweis überlassen.
- **Nutzer verwaister Software**. Millionen funktionierender Apps haben Entwickler, die unerreichbar, im Ruhestand oder verstorben sind. Diese Apps verschwinden nicht allmählich – sie werden blockiert. Es entsteht eine neue Kategorie: die **administrative Obsoleszenz** – funktionierende Software, getötet durch Bürokratie.
- **Das Reparatur- und Wiederverwendungs-Ökosystem** – bereits 2019 durch das Werbeverbot getroffen und nun ein zweites Mal: Gemeinschaften, die alte Hardware am Leben erhalten, sind auf frei installierbare Software angewiesen. Wird diese gelähmt, bricht auch der Nutzen der Geräte-Lebensverlängerung zusammen.

Ob diese Zielgenauigkeit Absicht oder Fahrlässigkeit ist, ist fast nebensächlich. Die Regelung ist passgenau so geformt, dass sie die Etablierten verschont und die Allmende belastet.

Gegen die Obsoleszenz – Optionen, solange die Tür noch offen ist

Bis zum Beginn der Durchsetzung verbleiben Nutzern und Gemeinschaften wirksame Optionen. Jetzt zu handeln ist entscheidend:

- **Archivieren Sie die Software, auf die Sie angewiesen sind**. Bewahren Sie lokale Kopien der APK-Dateien wichtiger Apps auf, insbesondere von Nischen- und Community-Werkzeugen, die voraussichtlich nie neu registriert werden.

- **Installieren Sie jetzt Custom-ROMs auf älteren Geräten.** Projekte wie LineageOS, GrapheneOS und /e/OS erscheinen ohne Googles Zertifizierungsschicht und unterliegen auf ihren eigenen Builds nicht der geräteseitigen Verifikationskontrolle. Ein heute geflashtes Gerät ist ein befreites Gerät.
- **Unterstützen Sie F-Droid und unabhängige Repositories** – finanziell und durch Mitarbeit – als Kerninfrastruktur des unkontrollierten Ökosystems.
- **Bevorzugen Sie Progressive Web Apps (PWAs)**, wo möglich; der Browser bleibt ein Verbreitungskanal, den Google nicht auf dieselbe Weise verriegeln kann.
- **Kaufen oder verwenden Sie Hardware mit entsperrbarem Bootloader** und belohnen Sie mit Ihrer Kaufentscheidung Hersteller, die dies erlauben.
- **Unterstützen Sie unabhängige Reparaturbetriebe** – direkt, vor Ort, unabhängig von ihrer Sichtbarkeit in Online-Werbekanälen, die ihnen seit 2019 versperrt sein können.
- **Unterstützen Sie regulatorischen Druck.** Der Digital Markets Act der EU adressiert ausdrücklich die Türwächter-Kontrolle über App-Installationen; Beschwerden – wie sie betroffene Reparaturbetriebe schon 2019 bei Wettbewerbszentrale, Bundeskartellamt und EU-Kommission einreichen –, Stellungnahmen in Konsultationen und die Unterstützung von Digital-Rights-Organisationen (FSFE, EFF, die Advocacy-Arbeit von F-Droid) sind konkrete Hebel.
- **Für Entwickler: Veröffentlichen Sie jetzt Quellcode und reproduzierbare Builds**, damit Gemeinschaften die Software weiterpflegen und neu signieren können, selbst wenn der ursprüngliche Autor sich nie registriert.

Nichts davon ersetzt eine offene Plattform vollständig. Es sind Milderungsmaßnahmen – Sandsäcke vor einer Flut.

Die Umweltrechnung: Eine Schätzung

Der Zusammenhang zwischen Softwarefreiheit und Elektroschrott ist direkt: **Die Nutzungsdauer eines Geräts endet, wenn es die Software nicht mehr ausführen kann, die sein Besitzer benötigt.** Die Einschränkung unabhängiger Software verkürzt diese Dauer. Was kostet das global?

Die folgende Schätzung legt ihre Annahmen offen und ist als Größenordnungsrechnung zu lesen, nicht als präzise Prognose:

Annahmen:

- Rund 3 Milliarden aktive Android-Geräte weltweit.
- Umfragedaten legen nahe, dass ein nennenswerter Anteil der Android-Nutzer Apps seitlich installiert oder Geräte über den offiziellen Support hinaus verwendet; allein Community-ROMs verzeichnen Millionen Installationen, Zweitmarkt- und

umgenutzte Geräte kommen hinzu. Konservativ angenommen: **3–8% des Gerätebestands** (90–240 Millionen Geräte) verdanken ihre verlängerte Nutzungsdauer wesentlich frei installierbarer Software.

- Angenommen, die neue Politik verkürzt die effektive Lebensdauer dieser Geräte um **durchschnittlich ein Jahr** (von etwa 5–7 Jahren verlängerter Nutzung zurück in Richtung des üblichen 3–4-Jahres-Zyklus) und zieht damit Ersatzkäufe vor.

Resultierender Abfall:

- **Zusätzlich vorzeitig entsorgte Geräte über den Übergangszeitraum: grob 50–150 Millionen.**
- Bei durchschnittlich etwa 180 Gramm pro Smartphone sind das **9.000–27.000 Tonnen direkter Geräte-Elektroschrott** – noch ohne Ladegeräte, Hüllen und Verpackungen, die diese Zahl verdoppeln können.
- Die tieferen Kosten liegen in der Produktionskette: Die Herstellung eines einzigen Smartphones verursacht in der Größenordnung von **55–80 kg CO₂-Äquivalent** (rund 80% des gesamten Lebenszyklus-Fußabdrucks) und erfordert den Abbau von Dutzenden Kilogramm Erz für die enthaltenen Metalle. 50 bis 150 Millionen vorgezogene Ersatzkäufe bedeuten daher **3–12 Millionen Tonnen zusätzliches CO₂-Äquivalent** und eine entsprechende Ausweitung des Abbaus von Kobalt, Lithium, Seltenen Erden und Gold – vielfach in ökologisch und sozial fragilen Regionen.
- Zur Einordnung: Smartphones tragen bereits erheblich zu den weltweit rund 62 Millionen Tonnen Elektroschrott pro Jahr bei, von denen **weniger als ein Viertel** formal recycelt wird. Die meisten dieser vorzeitig ausgemusterten Android-Geräte werden in Schubladen, auf Deponien oder in informellen Zerlegebetrieben des Globalen Südens enden.

Selbst vorsichtig gerechnet führt eine in Mountain View getroffene Konzernentscheidung zu **Zehntausenden Tonnen Elektroschrott und Millionen Tonnen CO₂** – die Umweltkosten tragen wir alle und sie tauchen in keiner Bilanz von Google auf¹. Und sie reiht sich ein in eine Politik, die schon 2019 ausgerechnet jene wirtschaftlich schwächte, die durch Reparaturen Ressourcen schonen: Marktbeobachter vermuteten bereits damals, dass ressourcenschonende Reparaturen von manchen Herstellern schlicht als entgangener Absatz von Neugeräten verstanden werden.

¹ **Anmerkung zu den Schätzungen:** Die Umweltzahlen in Abschnitt 6 sind szenariobasierte Berechnungen aus offengelegten Annahmen, keine gemessenen Ergebnisse – die tatsächlichen Auswirkungen hängen von den Details der Durchsetzung, von regulatorischen Eingriffen (insbesondere in der EU) und von der Anpassungsfähigkeit der Nutzerkreise ab.

Fazit: Die unbeglichene Schuld

Android existiert, weil Tausende Menschen ihre Arbeit einer Allmende schenkten – frei, auf Wunsch anonym, reguliert durch nichts als die Qualität ihres Codes. Dieses Erbe war Milliarden wert, und es war der Nährboden des am weitesten verbreiteten Betriebssystems der Erde. Das Mainstream-Linux hält diese Bedingungen bis heute ein.

Google hat nun entschieden, dass die Nutzer und kleinen Schöpfer dieses Ökosystems Bedingungen erfüllen müssen, denen das eigene Fundament nie unterlag: Zahle die Gebühr, unterschreibe die Bedingungen, zeige deine Papiere – oder deine Software läuft nirgendwo. Jede Etappe der Einhegung Androids wurde mit Sicherheit begründet, und jede Etappe festigte zufällig Kontrolle und Erträge – von der Aussperrung der unabhängigen Reparateure 2019 bis zur Registrierungspflicht für alle Entwickler 2026. Das Muster ist nicht mehr zu leugnen, und seine Kosten sind zählbar: in Software, die nie geschrieben werden wird, in verdrängten Gemeinschaften und Betrieben, in Geräten, die Jahre zu früh entsorgt werden, und in Bergen von Elektroschrott, die leise außer Sichtweite verschifft werden.

Die Tragik liegt nicht darin, dass ein Unternehmen an seiner Plattform verdient – Google verdient bereits prächtig an Hardware, App-Provisionen, Werbung und der fortlaufenden Ernte von Nutzerdaten. Die Tragik liegt in der Verwandlung einer Allmende in einen Kontrollposten – unter Verwendung eben jenes Systems, das durch freie Beiträge erst entstand. Was die Open-Source-Bewegung ohne Bedingungen gab, wird uns nun mit Bedingungen zurückverkauft – und das Zeitfenster, das Verbliebene zu bewahren, schließt sich nach einem Zeitplan, den Google bereits verkündet hat.

<https://keepandroidopen.org/de/>