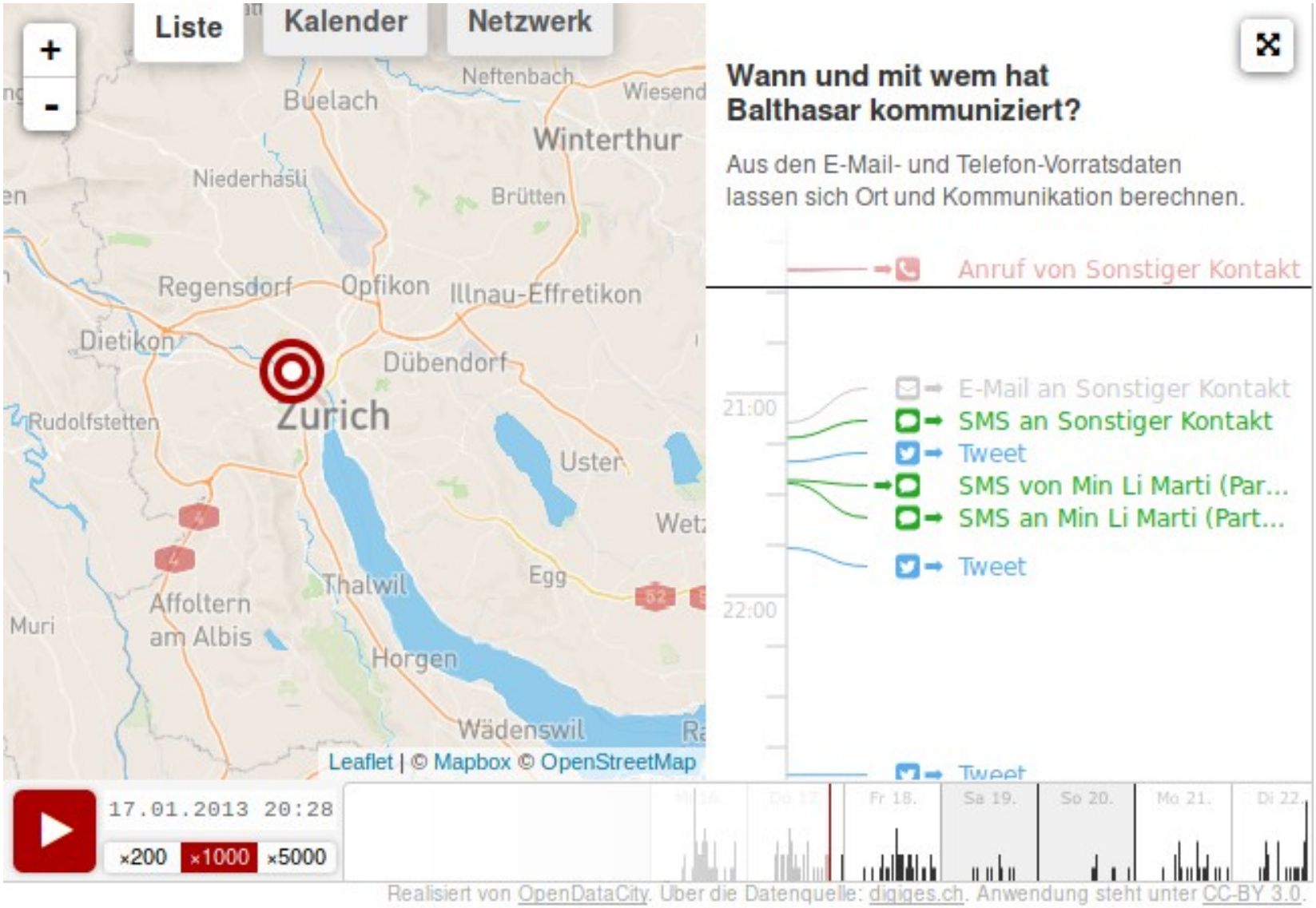
Mehr Privatsphäre aufs Smartphone

Bild von Andy Makely, unsplash.com

Das Smartphone: Dreh- und Angelpunkt für Datensammlungen

- Der Alltag spielt sich immer häufiger mit und auf dem Smartphone ab
- Das Smartphone als "externes Gehirn"
  - Die ständige Interaktion mit dem Gerät macht die Nutzer.in besonders transparent
- Smartphones sind als Konsumgeräte konzipiert
- Hardware („Super-Wanze“)
  - Mikrofone, Kameras, GPS, Bewegungssensoren…
- Welche Grenzen setzt das Betriebssystem?

Verräterisches Telefon

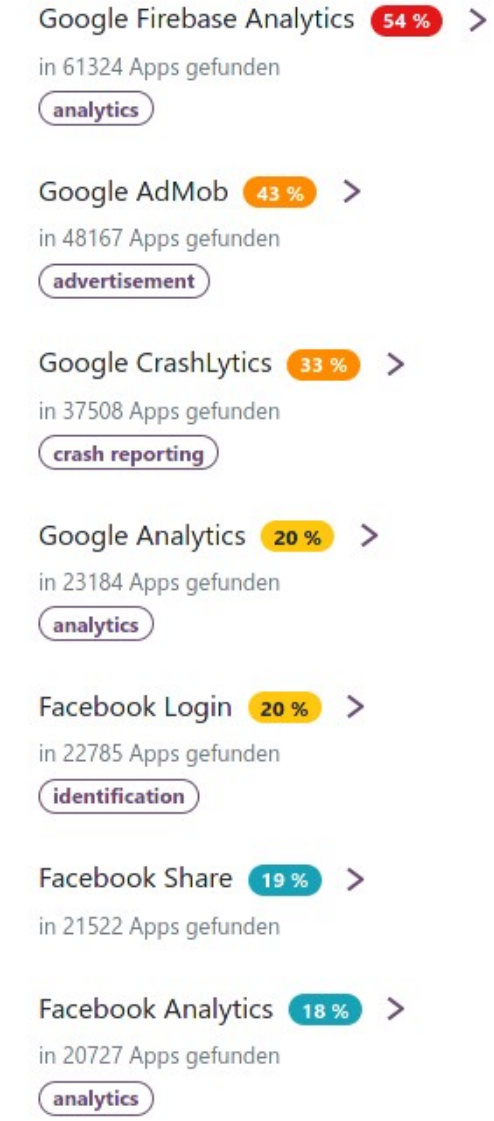


Was ist Tracking?

- Das Verfolgen von Nutzer.innen über Websites und Anwendungen hinweg
- Erstellung von Nutzungsprofilen, um z. B. je nach Standort, Interessen und Gewohnheiten der Person passende Werbung auszuspielen
- Datenerfassung in der Regel „unsichtbar“
- Im Browser z. B. über Cookies, Fingerprinting, Cache...

Wie funktioniert Tracking in Apps?

- Einbau von Modulen/Bibliotheken größerer Anbieter, um z. B. Gerätedaten zu sammeln, Verhalten zu analysieren oder Werbung auszuliefern
  - Wer welche Daten zu welchem Zweck sammelt, ist für Nutzer.innen kaum transparent
  - Legitime Anliegen häufig nicht von übergriffigem Verhalten zu unterscheiden
- Statische Werbe-ID von Google oder Apple als eindeutiges Erkennungsmerkmal
  - Lässt sich zurücksetzen: https://mobilsicher.de/ratgeber/smartphone-nutzer-sollten-jetzt-ihre-werbe-id-aendern



iOS: Vermeintlicher Datenschutzengel

- Apple fährt seit einigen Jahren eine Kampagne als Verfechter von Privatsphäre, Sicherheit und Datenschutz:
  - Verweigern der Mithilfe beim Entsperren von verschlüsselten iPhones
  - Ausbau des Trackingschutzes in iOS
  - Strikte Kontrolle des eigenen Ökosystems
  - „Was auf deinem iPhone passiert, bleibt auf deinem iPhone.“

iOS

Bildquellen: https://commons.wikimedia.org/wiki/File:IOS_wordmark_(2017).svg
https://9to5mac.com/2019/01/05/apple-privacy-billboard-vegas-ces/

iOS: Vermeintlicher Datenschutzengel

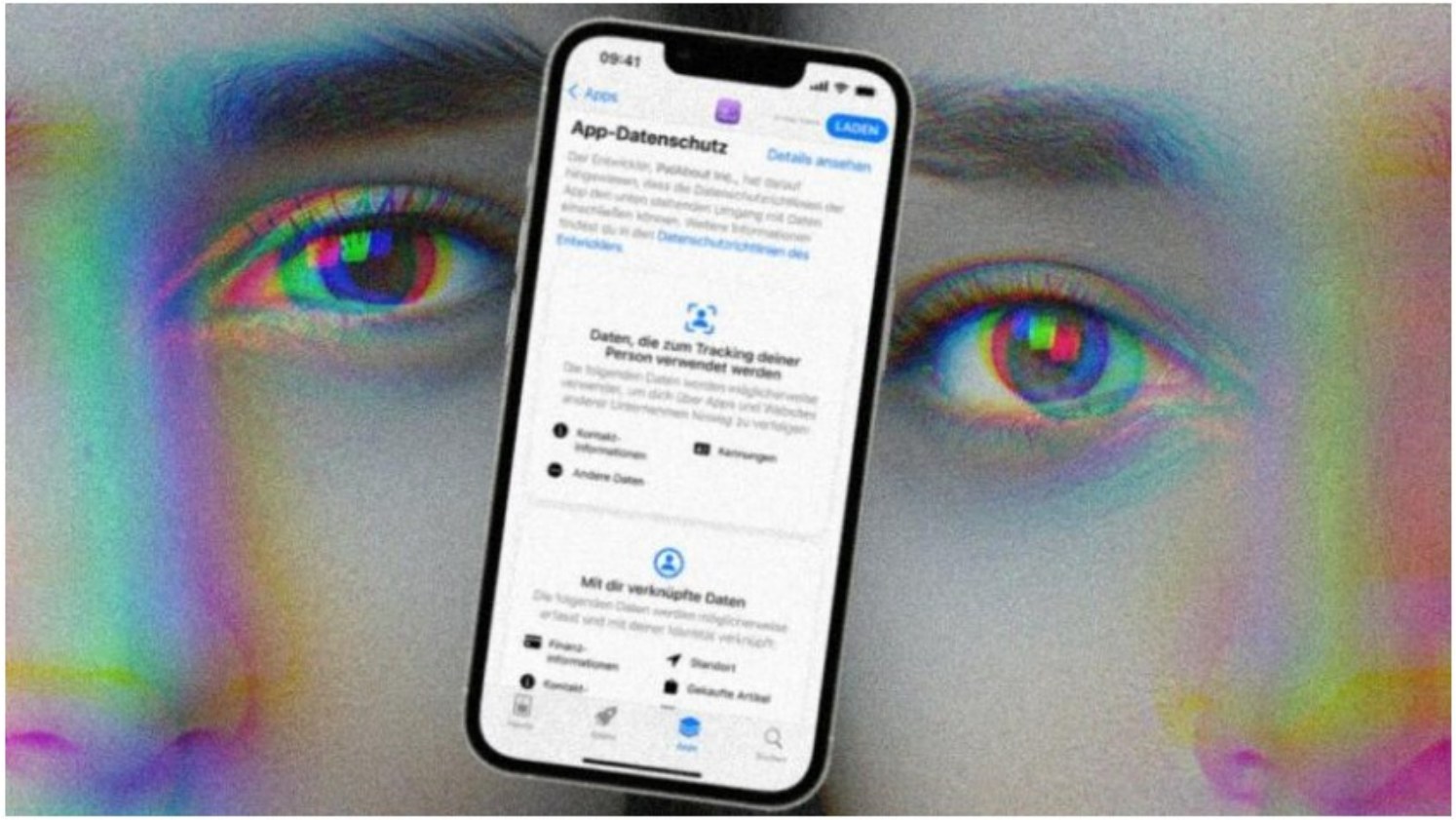
- Die Kehrseiten...
  - Die Geräteverschlüsselung konnte ausgehebelt werden, Quellcode von Apples Software nicht offen und Sicherheit daher nicht unabhängig überprüfbar
  - Neuer Trackingschutz in iOS, Sperrung des Zugriffs auf Werbe-ID
    - Tracking geschieht trotzdem! https://www.washingtonpost.com/technology/2021/09/23/iphone-tracking/
  - Strikte Kontrolle des eigenen Ökosystems:
    - Wenig bis gar kein Raum für alternative Plattformen und freie Software, Apple diktiert Vorgaben im Guten wie im Schlechten
  - Scans von Fotobibliotheken und Nachrichten in Planung, derzeit verschoben (Mails werden bereits seit 2019 gescannt)
  - Edward Snowden: "Apple hat der Privatsphäre den Krieg erklärt"

Apple-Datenschutzlabels

Großteil angeblich trackingfreier iOS-Apps sammelt heimlich Daten

Apps auf dem iPhone tragen leicht verständliche Labels, die zeigen sollen, auf welche Daten sie zugreifen. Doch bei 80 Prozent der untersuchten Apps, die angeblich keine Daten erfassen, findet doch Tracking statt. Das zeigt eine Analyse des Informatikers Konrad Kollnig für netzpolitik.org.

20.01.2022 um 08:00 Uhr - Alexander Fanta - in Datenschutz - keine Ergänzungen



Bildquelle:
https://netzpolitik.org/2022/apple-datenschutzlabels-grossteil-angeblich-trackingfreier-ios-apps-sammelt-heimlich-daten/

Android:

- Theoretisch gute Basis …
  - Linux-basiert, im Kern freie Software

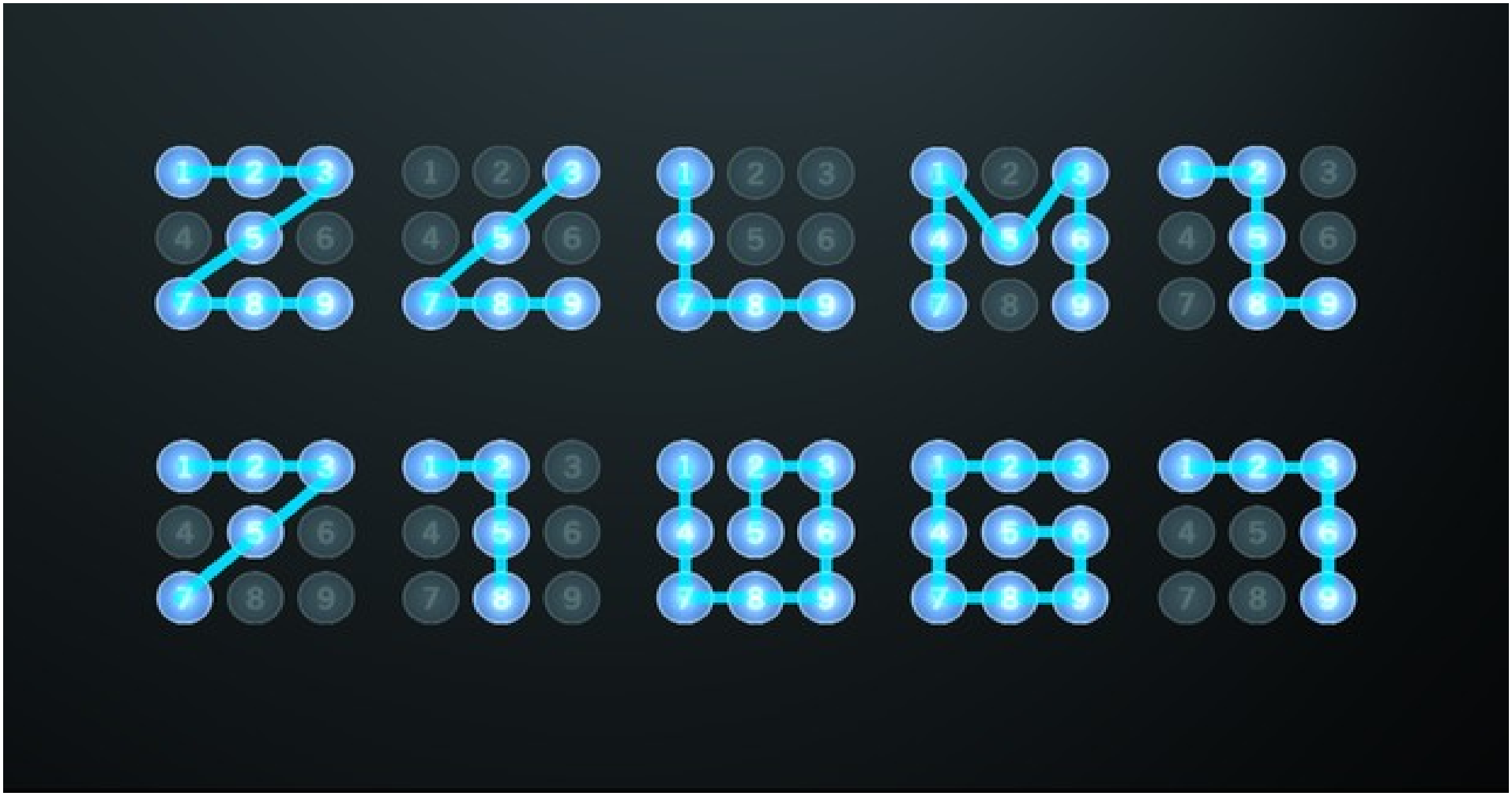
- **Aber:**
  - Google-Dienste und andere unfreie Komponenten/Apps
  - Nutzer wird zur Einrichtung eines (Google-)Kontos gedrängt
  - Fernzugriff, Datenübermittlung
  - Standardmäßig keine Gerätehoheit
  - Oft unzureichende Versorgung mit Sicherheitsupdates durch den Hersteller, starke Abhängigkeit von Google

Bildquelle: https://commons.wikimedia.org/wiki/File:Android_robot_head.svg

Wie kommt mehr Privatsphäre aufs Smartphone?

- Schrittweises Vorgehen:
  - Grundsätzliche Systemeinstellungen verbessern
  - "App-Minimalismus"
    - Bisher installierte und neue Apps prüfen und bewusst auswählen
    - Berechtigungen einschränken
    - Freie Alternativen nutzen
  - Werbe-/Tracking-/Inhaltsblocker nutzen

Typische Wischgesten



Erste Schritte: Konfiguration

- Sichere Bildschirmsperre
  - von unsicher zu sicher:
    Wischgeste, Muster, Biometrisch, PIN, Passwort
- Benachrichtigungsinhalte auf dem Sperrbildschirm verbergen
- Gerätespeicher verschlüsseln (auf neueren Geräten Standard)
- WLAN, GPS, Bluetooth, etc. ausschalten, wenn nicht genutzt
- Digitalen Assistenten (Google Assistant, Siri) abschalten
- Details zu allen Punkten auf dem Handout!

App-Berechtigungen: Facebook (1)

- Geräte- & App-Verlauf
  - Aktive Apps abrufen
- Identität
  - Konten auf dem Gerät suchen
  - Konten hinzufügen oder entfernen
  - Kontaktkarten lesen
- Kalender
  - Kalendertermine sowie vertrauliche Informationen lesen
  - Ohne Wissen der Eigentümer Kalendertermine hinzufügen oder ändern und E-Mails an Gäste senden
- Kontakte
  - Konten auf dem Gerät suchen
  - Kontakte lesen
  - Kontakte ändern

App-Berechtigungen: Facebook (2)

- Standort
  - Ungefährer Standort (netzwerkbasiert)
  - Genauer Standort (GPS- und netzwerkbasiert)
- SMS
  - SMS oder MMS lesen
- Telefon
  - Telefonstatus und Identität abrufen
- Anrufliste lesen
  - Anrufliste bearbeiten
- Fotos/Medien/Dateien
  - USB-Speicherinhalte lesen
  - USB-Speicherinhalte ändern oder löschen
- Speicher
  - USB-Speicherinhalte lesen
  - USB-Speicherinhalte ändern oder löschen

App-Berechtigungen: Facebook (3)

- Kamera
  - Bilder und Videos aufzeichnen
- Mikrofon
  - Ton aufzeichnen
- WLAN-Verbindungsinformationen
  - WLAN-Verbindungen abrufen
- Geräte-ID & Anrufinformationen
  - Telefonstatus und Identität

App-Berechtigungen: Facebook (4)

- Sonstige
  - Dateien ohne Benachrichtigung herunterladen
  - Größe des Hintergrundbildes anpassen
  - Daten aus dem Internet abrufen
  - Netzwerkverbindungen abrufen
  - Konten erstellen und Passwörter festlegen
  - Akkudaten lesen
  - dauerhaften Broadcast senden
  - Netzwerkkonnektivität ändern
  - WLAN-Verbindungen herstellen und trennen
  - Statusleiste ein-/ausblenden
  - Zugriff auf alle Netzwerke
  - Audio-Einstellungen ändern
  - Synchronisierungseinstellungen lesen
  - Beim Start ausführen
  - Aktive Apps neu ordnen
  - Hintergrund festlegen
  - Über anderen Apps einblenden
  - Vibrationsalarm steuern
  - Ruhezustand deaktivieren
  - Synchronisierung aktivieren oder deaktivieren
  - Verknüpfungen installieren
  - Google-Servicekonfiguration lesen

Kommerzielle Datensammlungen über Apps

- Smartphones bieten einen umfassenden Markt für optimierte personenbezogene Werbung
- Beispiel: Die Diabetiker-App **mySugr** übermittelte in einem Test von Mike Kuketz u.a. folgende Daten an das US-Unternehmen Mixpanel
  - E-Mail-Adresse
  - Vor- und Nachname der Person
  - Diabetes-Typ
  - Art der Therapie (Spritze oder Pumpe)

Kriterien für vertrauenswürdige Apps

1) Sie ist quelloffen.
2) Sie ist reproduzierbar.
3) Sie enthält keine Tracker.
4) Sie arbeitet möglichst datensparsam.
5) Sie zwingt nicht zur Benutzung eines bestimmten App-Stores.
6) Kein Registrierungszwang.
7) Sie hält sich an geltendes Recht.

https://digitalcourage.de/digitale-selbstverteidigung/app-kriterien

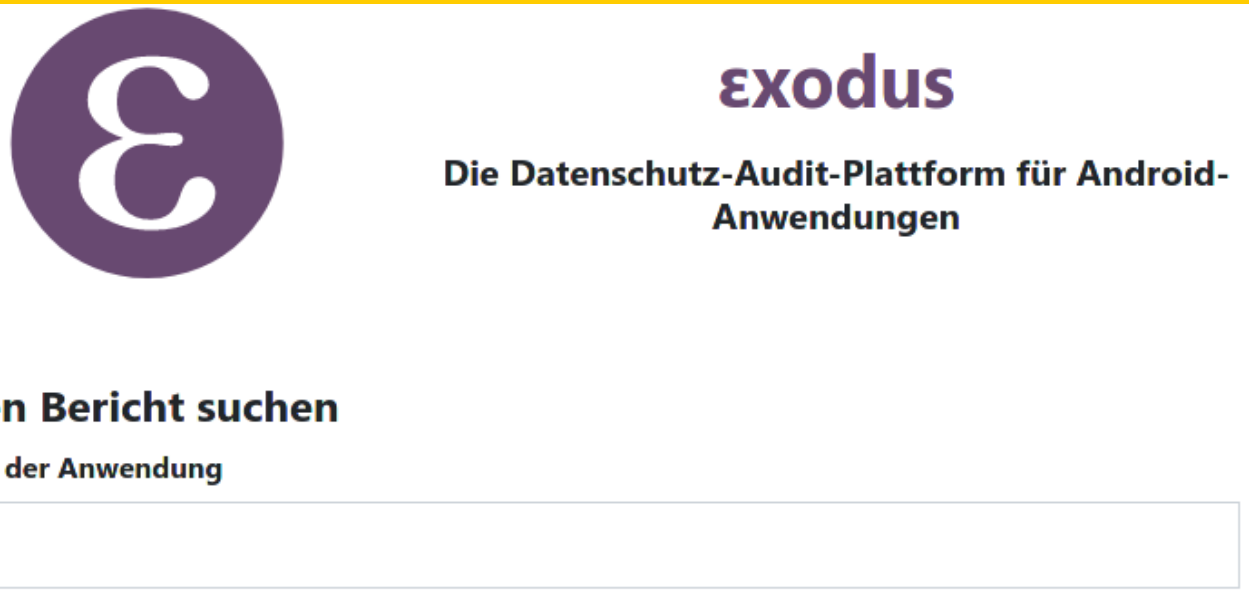
„Gute“ und „böse“ Apps unterscheiden: Kritischer Umgang mit Apps

- „Kostenlose“ Apps im App/Play Store verdienen häufig mit Datensammelei und Werbung an den Nutzer.innen
  - Aber: Auch Bezahl-Apps operieren nicht ohne Datensammlung
  - Geschäftsmodell hinterfragen: Wie finanziert sich der angebotene Dienst?
- Sich selbst hinterfragen: Braucht man diese App wirklich?
- Berechtigungen hinterfragen: Braucht die App diese oder jene Berechtigung für ihre Funktion überhaupt?
- Gibt es alternativ eine Website, die man nutzen kann?
- Arbeiten funktional vergleichbare Apps datensparsamer?

„Gute“ und „böse“ Apps unterscheiden: Wie geht das?

- Die Datenschutzbestimmungen lesen
  - Leider nicht immer ehrlich und rechtskonform
- Store-Seiten und Webauftritte der jeweiligen Apps "abklopfen", externe Berichte/Tests lesen
- App-Verkehr mit Trackingblockern auslesen
  - Mehr dazu gleich
- App-Verkehr untersuchen (für Profis!)
  - Technisch aufwendig, Spezial-Tools notwendig, erfordert Know-How
- Android: Datenbank für automatisierte Tests durchsuchen
  - Exodus-Privacy

Übergriffige Apps aufdecken: Exodus Privacy (Android)



- Freier Analysedienst für Apps aus dem Play Store
  - Zu prüfende Apps müssen kostenlos und ohne regionale Einschränkungen im Play Store verfügbar sein
  - Als Indikator nutzen: tatsächliche Trackernutzung nicht zwingend
  - Auch als App verfügbar

    https://reports.exodus-privacy.eu.org/de/

Bilder (auch folgende Folie): Eigene Screenshots
https://reports.exodus-privacy.eu.org/

Lieferando

11 Tracker

12 Berechtigungen

Version 7.13.0 - andere Versionen anzeigen
Quelle: Google Play
Bericht erstellt am 2. November 2021 01:09

Auf Google Play anzeigen >

11 Tracker

Wir haben die **Code-Signatur** der folgenden Tracker in der Anwendung gefunden:

Adjust >
analytics

Facebook Analytics >
analytics

Facebook Login >
identification

Facebook Share >

Google AdMob >
advertisement

App-Berechtigungen einschränken:

- Entzug von Berechtigungen, um Zugriff auf sensible Daten zu verhindern
- Bei modernen Systemversionen werden Berechtigungen bei Benutzung der App von der Nutzer.in einzeln abgefragt
- Berechtigungen nachträglich ändern
  - Android: Einstellungen -> Apps & Benachrichtigungen

    -> App auswählen -> Berechtigungen oder: Erweitert -> Berechtigungsmanager
  - iOS: Einstellungen -> Datenschutz
    - Neu seit iOS 14: Kategorie "Tracking"
- Grundsätzlich: Apps und Berechtigungen immer wieder mal aufräumen!

Web-Apps (PWAs) nutzen

- Warum Web-Apps?
  - Unterliegen den den Einschränkungen des Browsers, keine ausufernden Trackingmöglichkeiten
- Firefox und Chromium für Android erlauben die Installation bestimmter Websites als Web-App ("Progressive Web App")
  - Aber: Tracking nicht grundsätzlich ausgeschlossen
  - Dezentral, kein Verzeichnis von Angeboten wie bei App-Stores
- Android: App mit dem Namen **WebApps**
  - Isoliert jede gewünschte Website in einem eigenen Browserfenster
  - https://github.com/tobykurien/WebApps

Freie App-Alternativen nutzen

- Freie Software wird in der Regel für die Nutzer.innen geschrieben, nicht für Konzerne
- Tracking sehr selten, dann oft deutlich transparenter
- Freie von „gewöhnlichen“ Apps in den App-Stores kaum von voneinander zu unterscheiden
- F-Droid als Alternativ-Store für freie Apps
- Einige App-Empfehlungen für Android: https://digitalcourage.de/fdroid

Freie Software

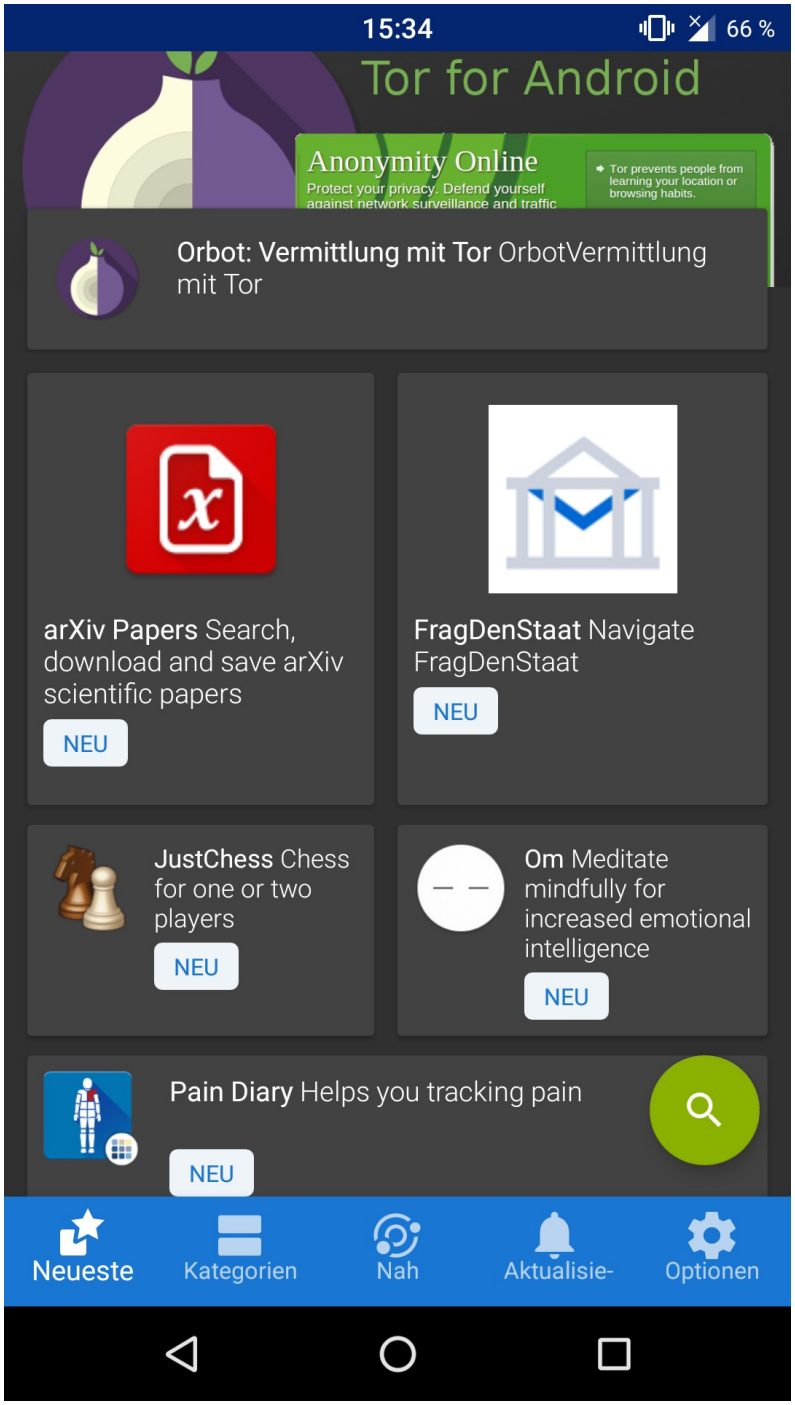
- **Freiheit 0**: Die Freiheit, das Programm auszuführen, wie man möchte, für *jeden Zweck.*
- **Freiheit 1**: Die Freiheit, die Funktionsweise des Programms zu untersuchen und eigenen Bedürfnissen der Datenverarbeitung anzupassen.
- **Freiheit 2**: Die Freiheit, das Programm weiterzuverbreiten und damit seinen Mitmenschen zu helfen.
- **Freiheit 3**: Die Freiheit, das Programm zu verbessern und diese Verbesserungen der Öffentlichkeit freizugeben, damit die gesamte Gemeinschaft davon profitiert.

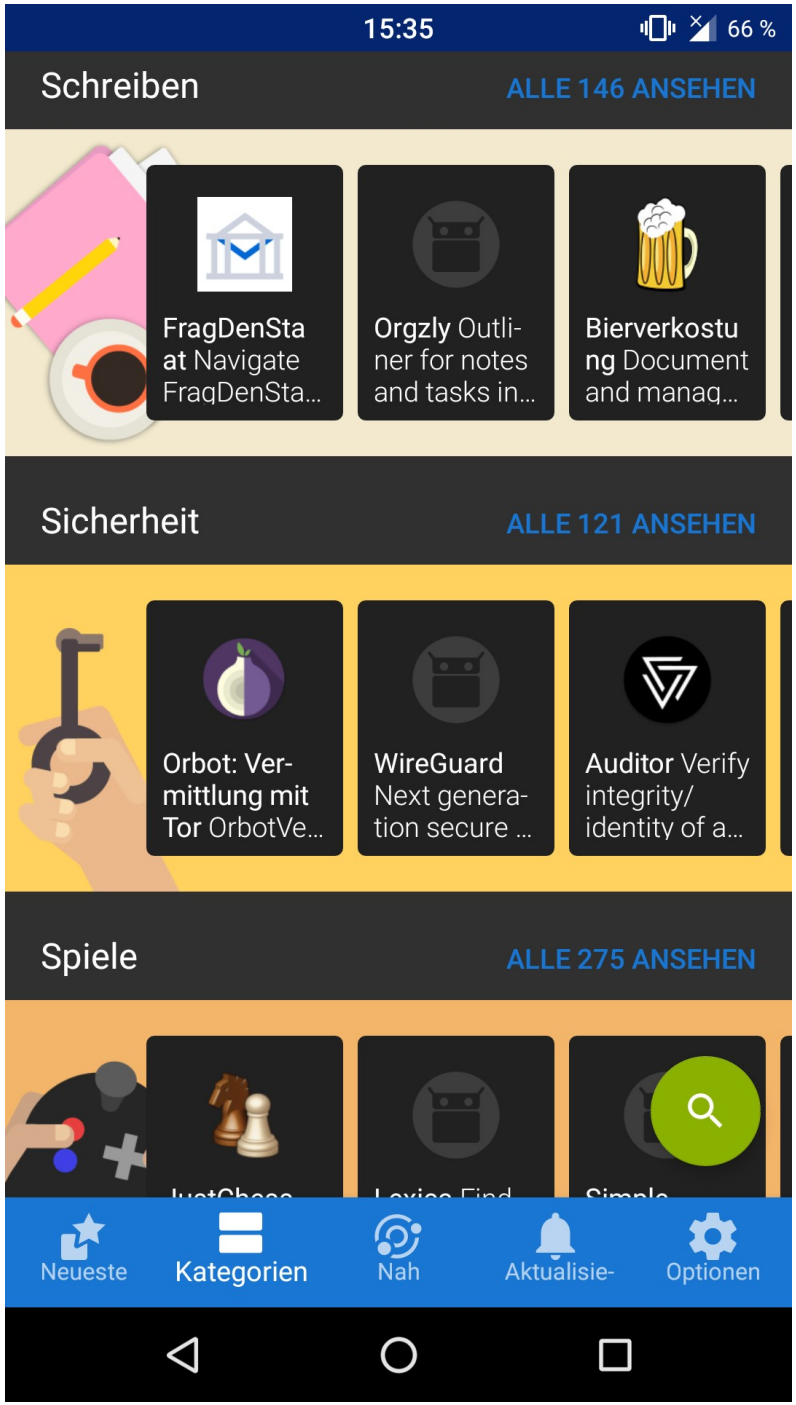
  → viel mehr als Open Source (Offenlegen der Quelltexte)

Empfehlenswerte Apps: F-Droid

- Alternative/Ergänzung zum Play Store: F-Droid
  - https://f-droid.org/
- Ausschließlich Software/Apps unter freier Lizenz
- Kein Nutzerkonto erforderlich
- Es ist möglich, eigene App-Repositories zur Verfügung zu stellen und einzubinden
- Auch direkter Download von Apps über die Website möglich (dann meist keine automatischen Updates)
- Achtung: Kein Jugendschutz!

Bildquelle: https://f-droid.org/





Bilder: Eigene Screenshots F-Droid

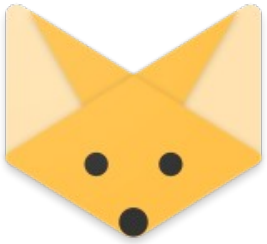
Alternative zu WhatsApp & Co.

- **Signal** (Android, iOS)

  - Freie Software
  - Sicherer Verschlüsselungsalgorithmus
  - Unterstützt verschlüsselte Text- und Sprachnachrichten und (Video-)Telefonie
  - Telefonnummer zwingend erforderlich, zentrale Struktur
  - Kostenlos im Play bzw. App Store, für Android auch als APK mit integriertem Updater: https://signal.org/android/apk/

Bilder: https://commons.wikimedia.org/wiki/File:Signal-Logo.svg

Empfehlenswerte Browser: Android



- **Mozilla Firefox / Fennec F-Droid**
  - Freie Software
  - unter Android durch Add-ons erweiterbar (z. B. uBlock Origin)
  - Konfiguration ähnlich zur Desktop-Version
  - iOS-Version stark eingeschränkt. Alternativ: **Firefox Klar**
- **Tor Browser** ebenfalls für Android verfügbar

Bildquellen: https://commons.wikimedia.org/wiki/File:Firefox_logo,_2019.svg, https://f-droid.org/

Empfehlenswerte Browser: iOS

- **Safari**
  - Vorinstalliert, tief ins System integriert
  - Keine freie Software
  - Teilweise gute Privatsphärefunktionen, Nachkonfiguration nötig
  - Apps wie **Firefox Klar** können als Inhaltsblocker genutzt werden (mehr dazu auf dem Handout)
- **Onion Browser** als Alternative zum Tor Browser

Bildquelle: https://en.wikipedia.org/wiki/File:Safari_14_icon.png

Weitere Apps für den Datenschutz (Android)

- **UntrackMe**
  - Leitet Links zu YouTube, Twitter, Instagram, Google Maps auf datenschutzfreundliche Dienste um
  - Nur bei F-Droid verfügbar.

- **Shelter**
  - Installiert oder klont Apps ins Arbeitsprofil
    - "Böse" Apps vom Rest des Systems isolieren
    - Apps mit verschiedenen Accounts nutzen

Bildquellen: https://f-droid.org/

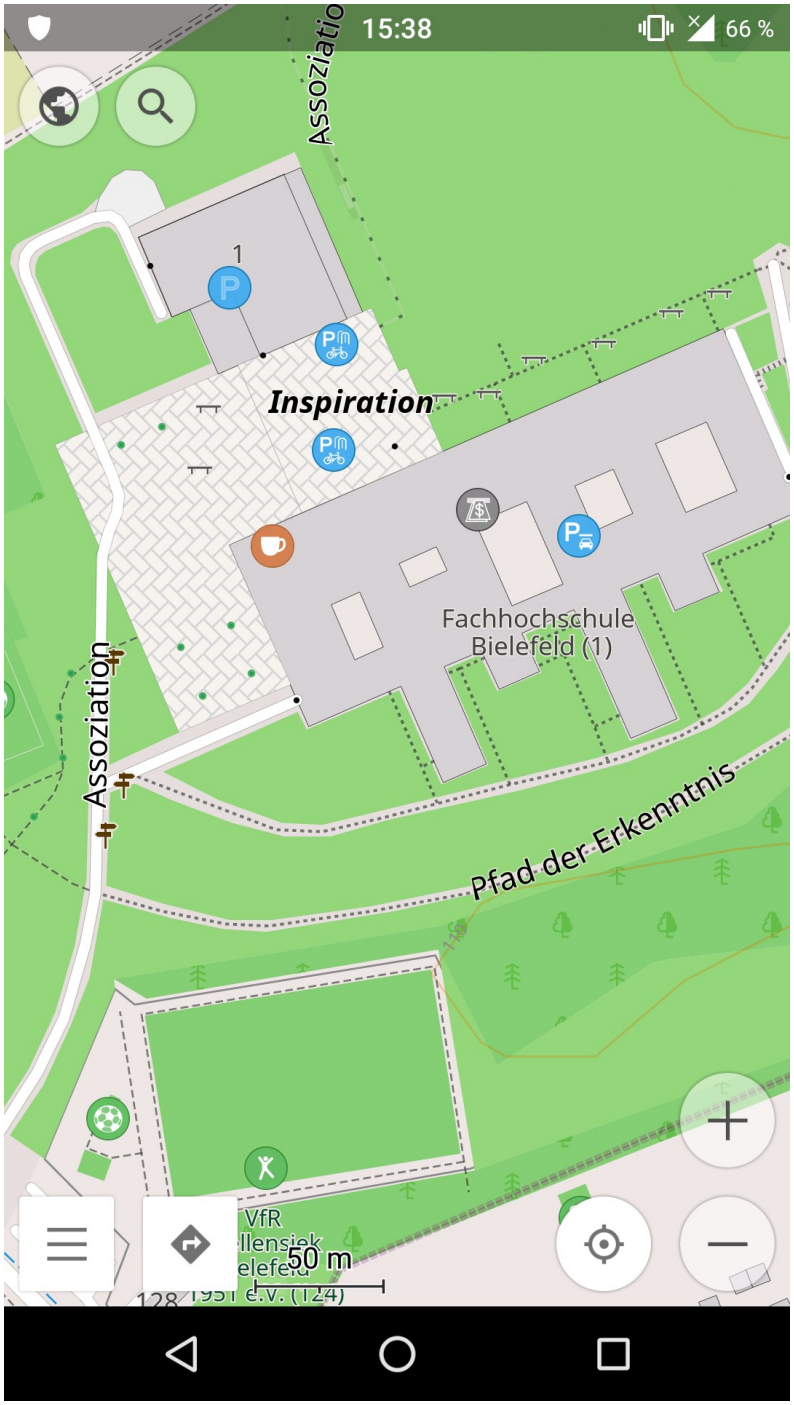
Beispiele für empfehlenswerte Apps

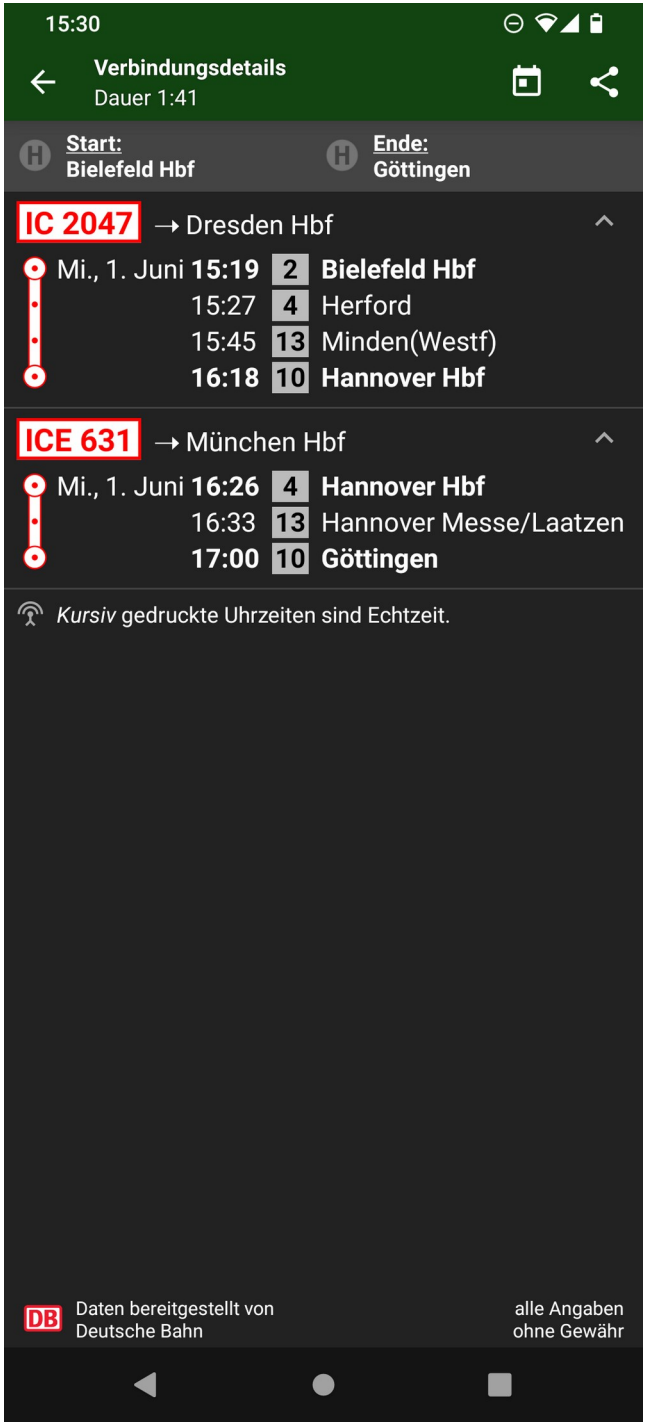
- **Öffi** (statt DB Navigator)
  - Fahrpläne des öffentlichen Nah-/Fernverkehrs & Verbindungssuche

- **VLC** (statt zahlloser anderer Mediaplayer-Apps)
  - Video- und Audioplayer

- **OsmAnd+** (statt Google Maps)
  - Karten- und Navigationssoftware auf Basis von OpenStreetMap, unterstützt auch Offline-Karten

Bildquellen: https://f-droid.org/





Bilder: Eigene Screenshots OsmAnd+, Transportr

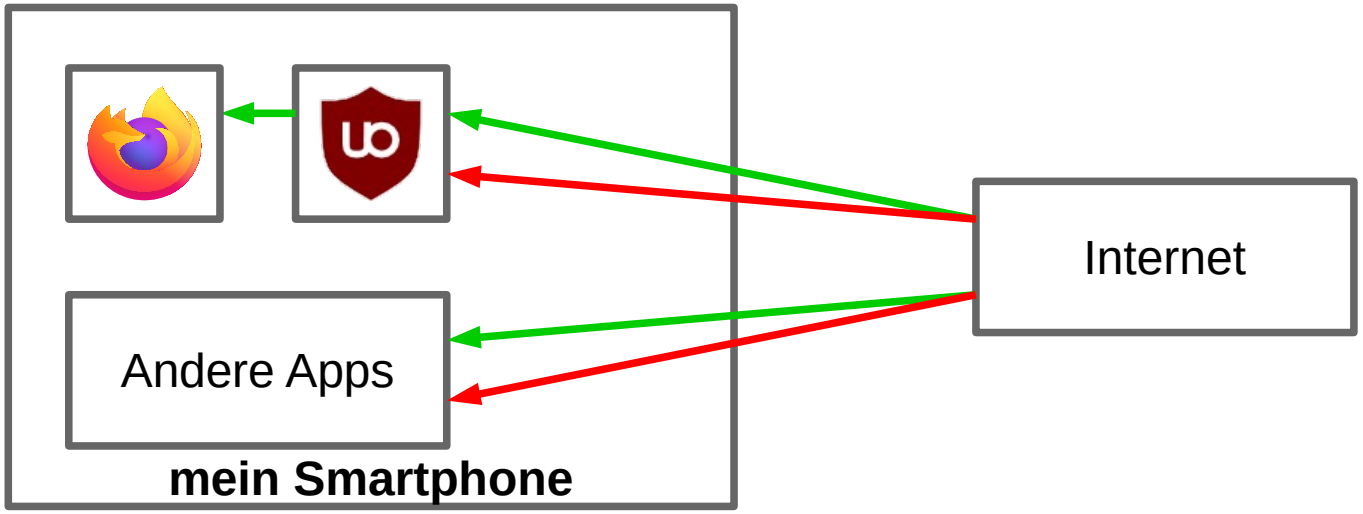
… und was ist mit Apps für iOS?

- Einige App-Empfehlungen:
  - **Collabora Office:** Office-Suite auf Basis von LibreOffice.
  - **Firefox Klar: Werbung und Tracking in Safari blockieren.**
  - **KeePassium:** Mit KeePassXC kompatible Passwortverwaltung.
  - **Onion Browser:** Webbrowser zum anonymen Surfen durch das Tor-Netzwerk.
  - **OsmAnd Maps Travel & Navigate:** Anwendung für Karten und Routenplanung, die auch offline funktioniert. Simplere Alternative: **Organic Maps**

    Mehr auf dem Handout!

Werbung auf Systemebene blockieren

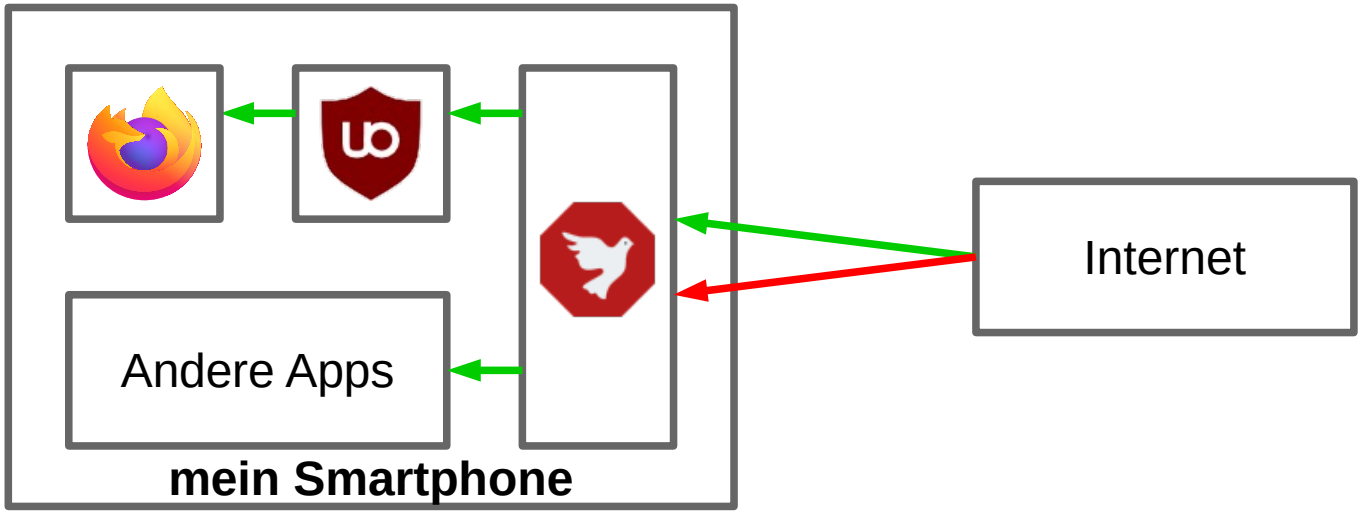
- Inhaltsblocker per Browser-Add-on ► wirkt nur im Browser
- Weiterhin Werbung in anderen Apps



Bildquellen: https://commons.wikimedia.org/wiki/File:Firefox_logo,_2019.svg, https://github.com/gorhill/uBlock

Werbung auf Systemebene blockieren

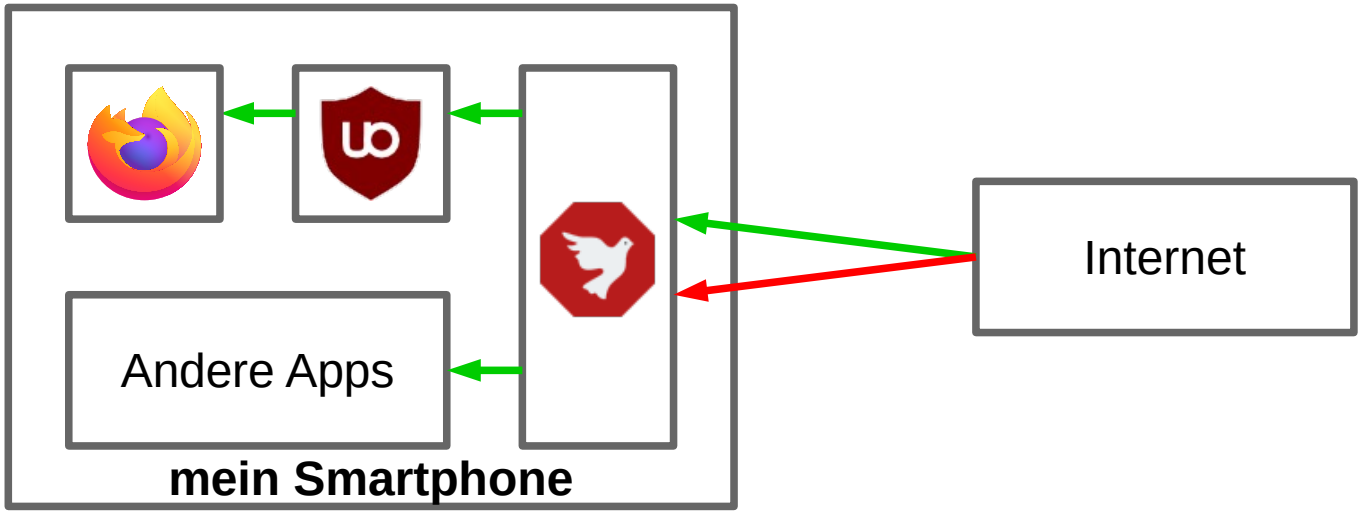
- App: Alle Verbindungen werden VPN-Schnittstelle gefiltert
- Werbung werden je nach Filterliste in (fast) allen Apps unterbunden
- Nicht mit anderen Diensten kompatibel, die die VPN-Schnittstelle nutzen (z.B. Orbot, OpenVPN, NetGuard)



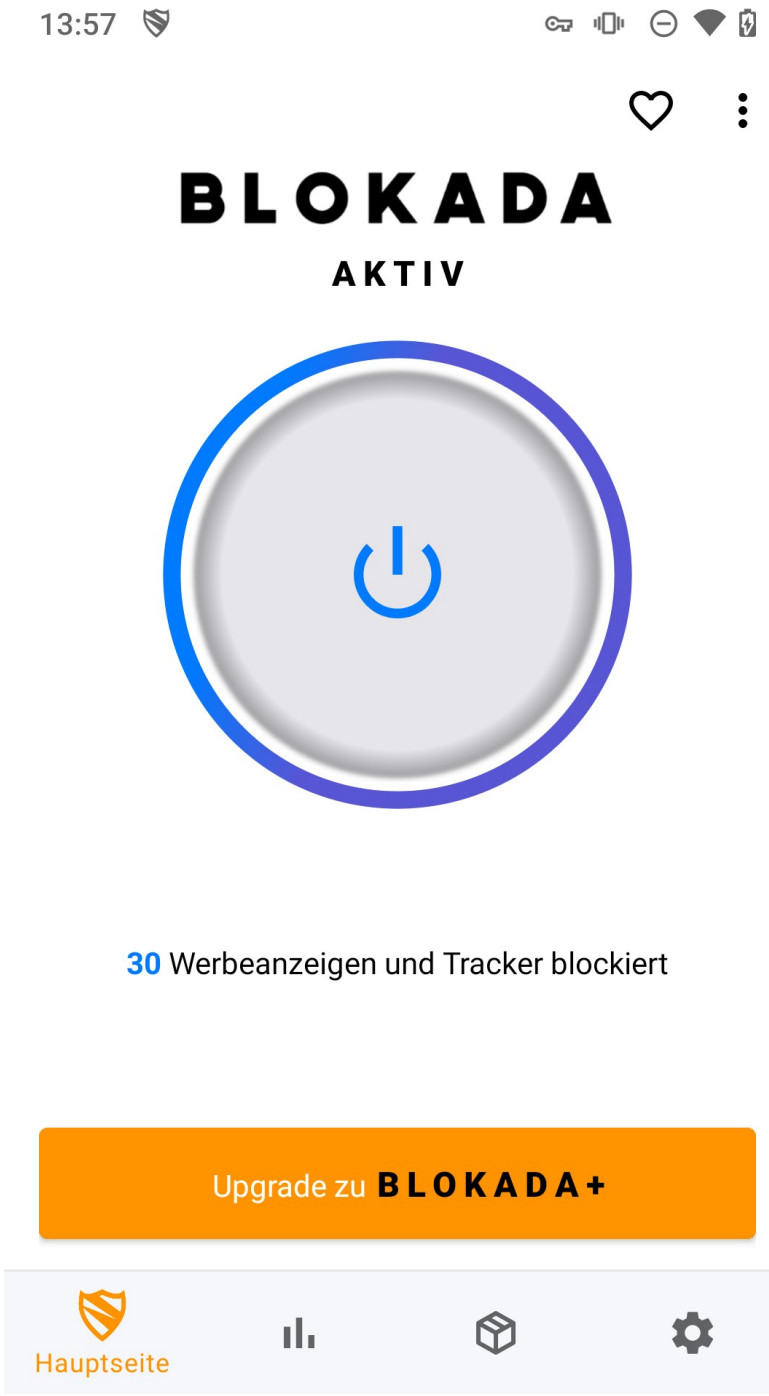
Bildquellen: https://commons.wikimedia.org/wiki/File:Firefox_logo,_2019.svg, https://github.com/gorhill/uBlock, https://f-droid.org/

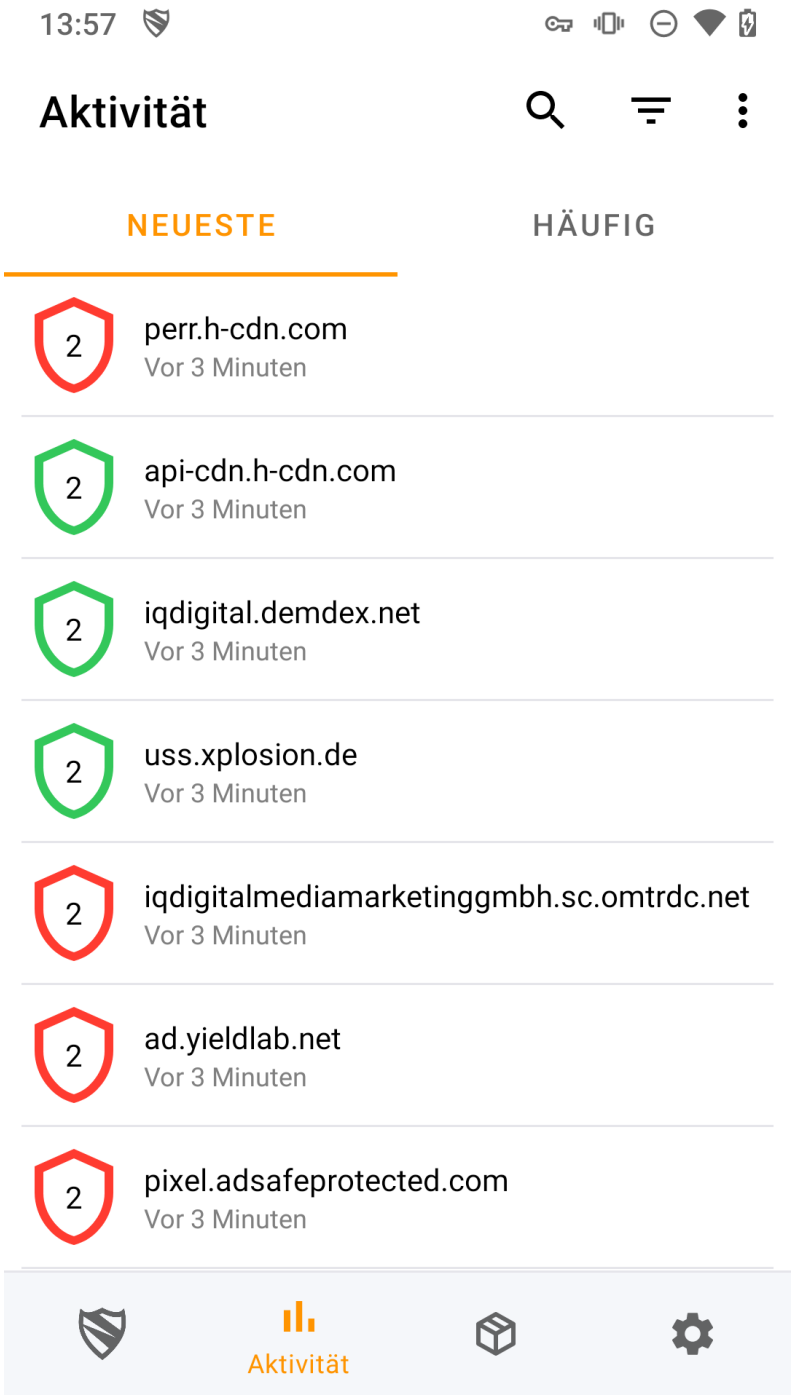
Werbung auf Systemebene blockieren

- Android **AdAway** über F-Droid oder als APK unter https://adaway.org/
  - Alternativen: **Blokada**, **TrackerControl**, **DNS66**, **NetGuard**
- Für iOS: **AdGuard Pro** (Bezahl-App)



Bildquellen: https://commons.wikimedia.org/wiki/File:Firefox_logo,_2019.svg, https://github.com/gorhill/uBlock, https://f-droid.org/

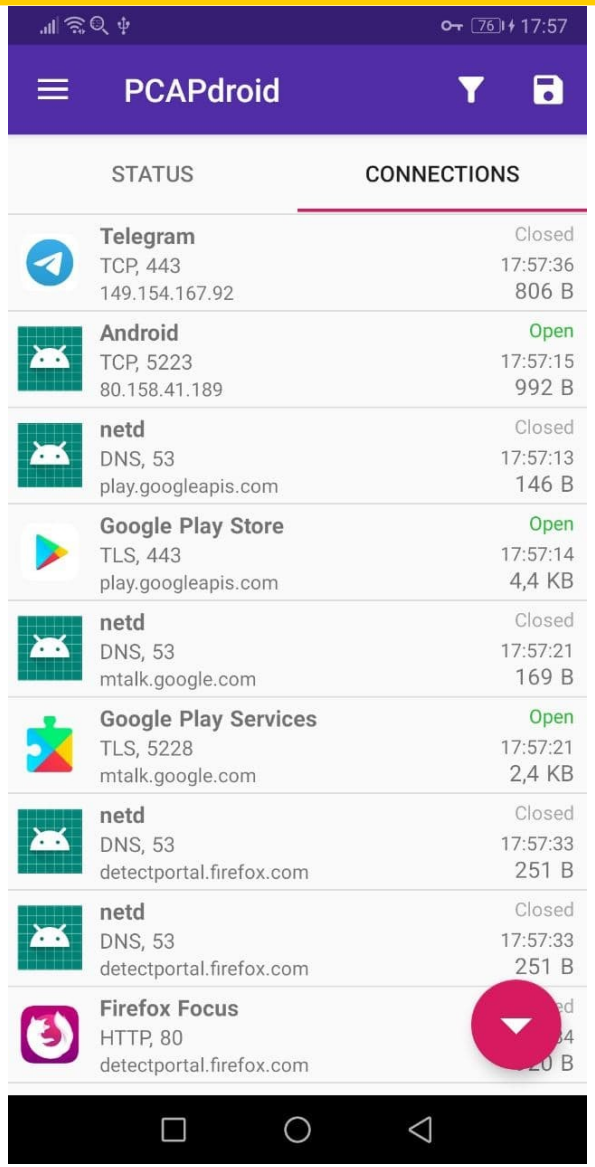

13:57
BLOKADA
AKTIV
30 Werbeanzeigen und Tracker blockiert
Upgrade zu BLOKADA+
Hauptseite


13:57
Aktivität
NEUESTE
HÄUFIG
2
perr.h-cdn.com
Vor 3 Minuten
2
api-cdn.h-cdn.com
Vor 3 Minuten
2
iqdigital.demdex.net
Vor 3 Minuten
2
uss.xplosion.de
Vor 3 Minuten
2
iqdigitalmediamarketinggmbh.sc.omtrdc.net
Vor 3 Minuten
2
ad.yieldlab.net
Vor 3 Minuten
2
pixel.adsafeprotected.com
Vor 3 Minuten
Aktivität

Datenverkehr auf Android auslesen

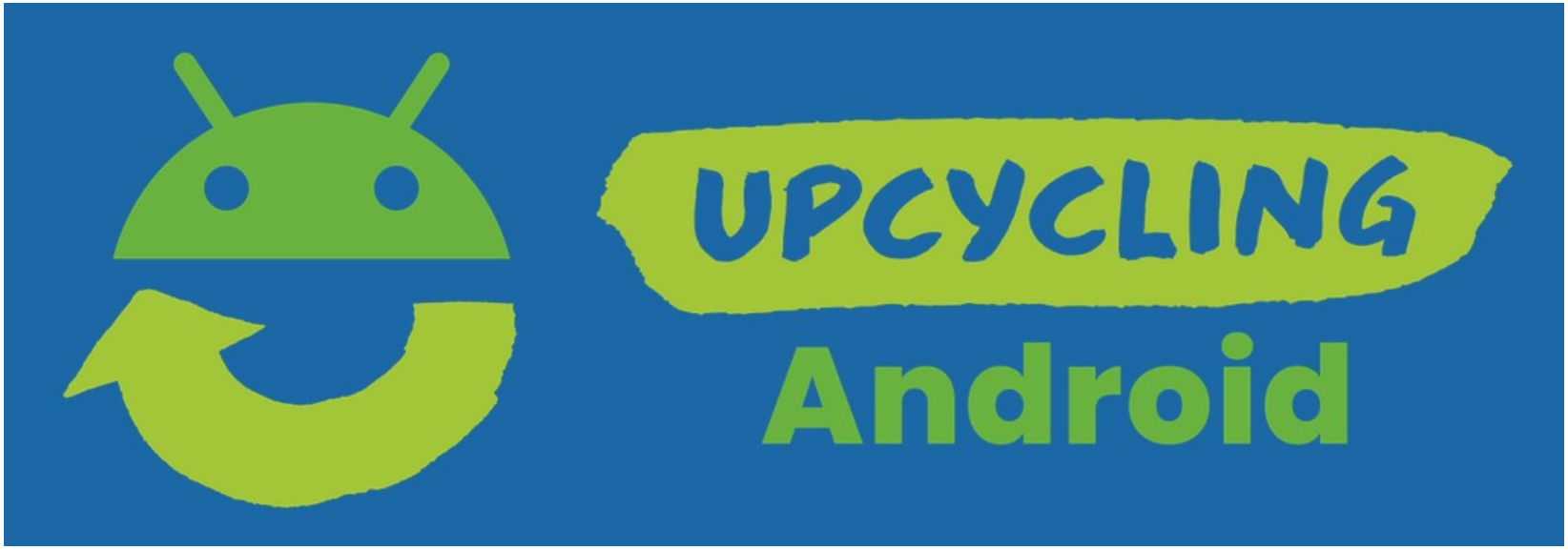
- **PCAP-Droid**

  - Nutzt die VPN-Schnittstelle von Android, um Datenverkehr von Apps aufzuzeichnen
  - Logs können durch externe Tools weiter analysiert werden
  - https://github.com/emanuele-f/PCAPdroid/



Bildquellen: https://github.com/emanuele-f/PCAPdroid/, https://f-droid.org/

Android-Smartphones länger nutzen



- Alte Android-Geräte können oft eigenhändig mit neueren Versionen des Betriebsystems versorgt werden, so dass sie länger genutzt werden können.
- Mehr Infos: https://fsfe.org/activities/upcyclingandroid/index.de.html

Bildquelle: https://fsfe.org/activities/upcyclingandroid/index.de.html

Exkurs:
Virenscanner auf dem Smartphone?

- Eigentlich sollte ein Virenscanner Schadsoftware fernhalten und damit Privatsphäre und Sicherheit schützen
- Notwendigkeit & Effektivität grundsätzlich fraglich, viele fragwürdige Apps offiziell in den Stores verfügbar
- Oft vollgestopft mit Trackern und sehr hohe Zahl an Berechtigungen
- Beitrag zur Notwendigkeit von Virenscannern auf Smartphones:
  - https://mobilsicher.de/ratgeber/schadprogramme-auf-dem-smartphone

Beispiel AVG Antivirus (Android)

Analyse bei Exodus Privacy:

Bilder: Eigene Screenshots vom Play Store, Exodus Privacy

Fazit

- Grundeinstellungen des Geräts durchgehen und konfigurieren, Browser sicher einrichten
- Apps auf Datenschutzfreundlichkeit überprüfen, sich auf Seiten wie z. B. mobilsicher.de informieren
- Kritischen Umgang mit der eigenen App-Nutzung entwickeln: Weniger ist mehr!
  - Nur Apps nutzen, auf die man wirklich nicht verzichten kann
  - Apps gut auswählen – freie Alternativen nutzen!
  - Berechtigungen prüfen und einschränken
- Werbe-/Trackingblocker (AdAway, AdGuard Pro) einsetzen, um Datenabfluss an Dritte zu unterbinden

Weiterführende Link-Hinweise & Literatur

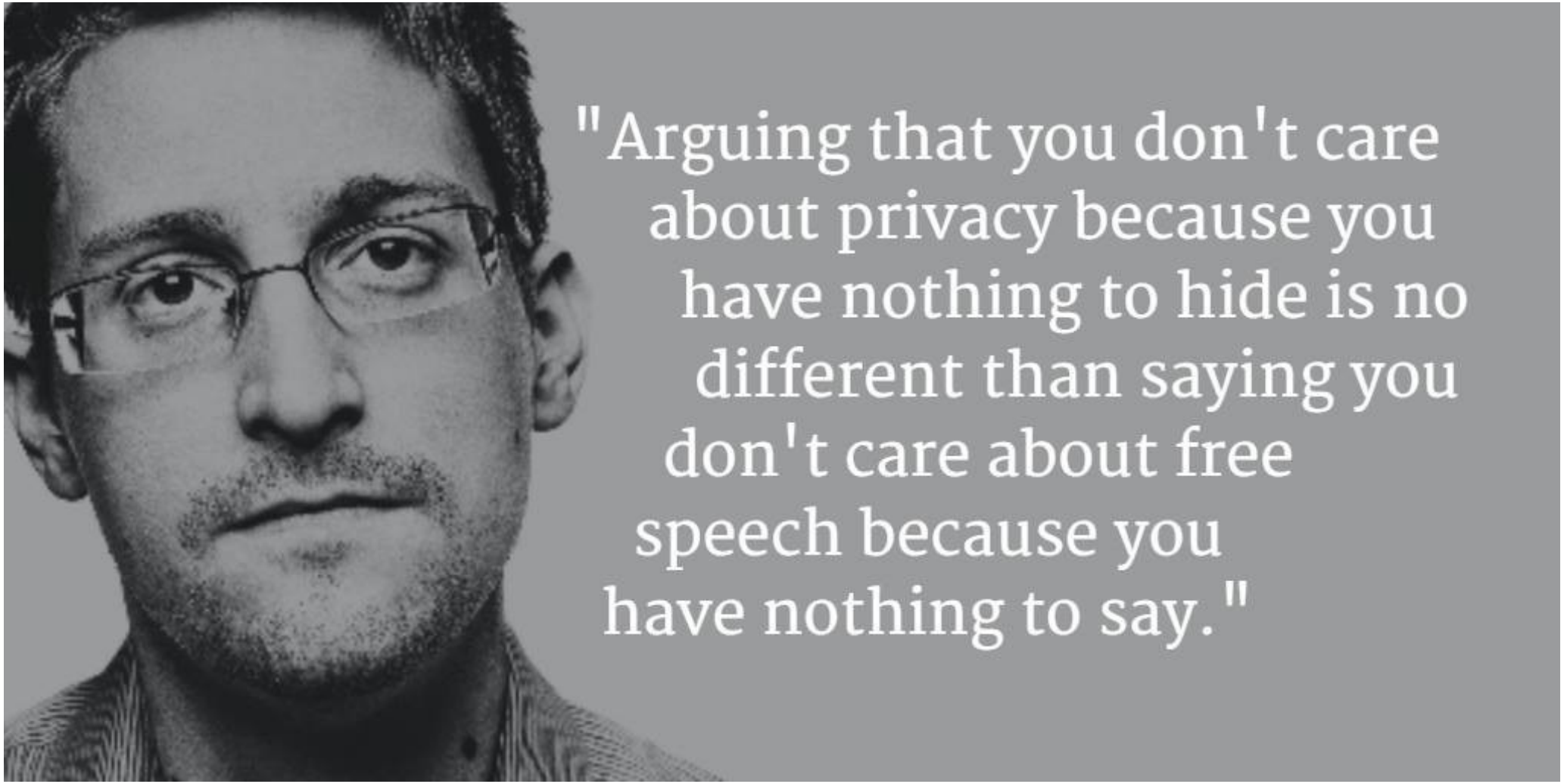
- **Blog von Mike Kuketz, Blog-Artikel & Empfehlungsecke**
  - https://www.kuketz-blog.de/
- **Mobilsicher.de**
  - https://mobilsicher.de/
- **Digitalcourage: Digitale Selbstverteidigung**
  - https://digitalcourage.de/digitale-selbstverteidigung/mobil
- Buchempfehlung: **Das Zeitalter des Überwachungskapitalismus** von Shoshana Zuboff

Zeit für Fragen und Diskussion

Falls die Zeit nicht mehr reicht:

jan.schoetteldreier@digitalcourage.de

Vielen Dank für Ihre Aufmerksamkeit!


"Arguing that you don't care about privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."