

Datenschutz auf Mobilgeräten

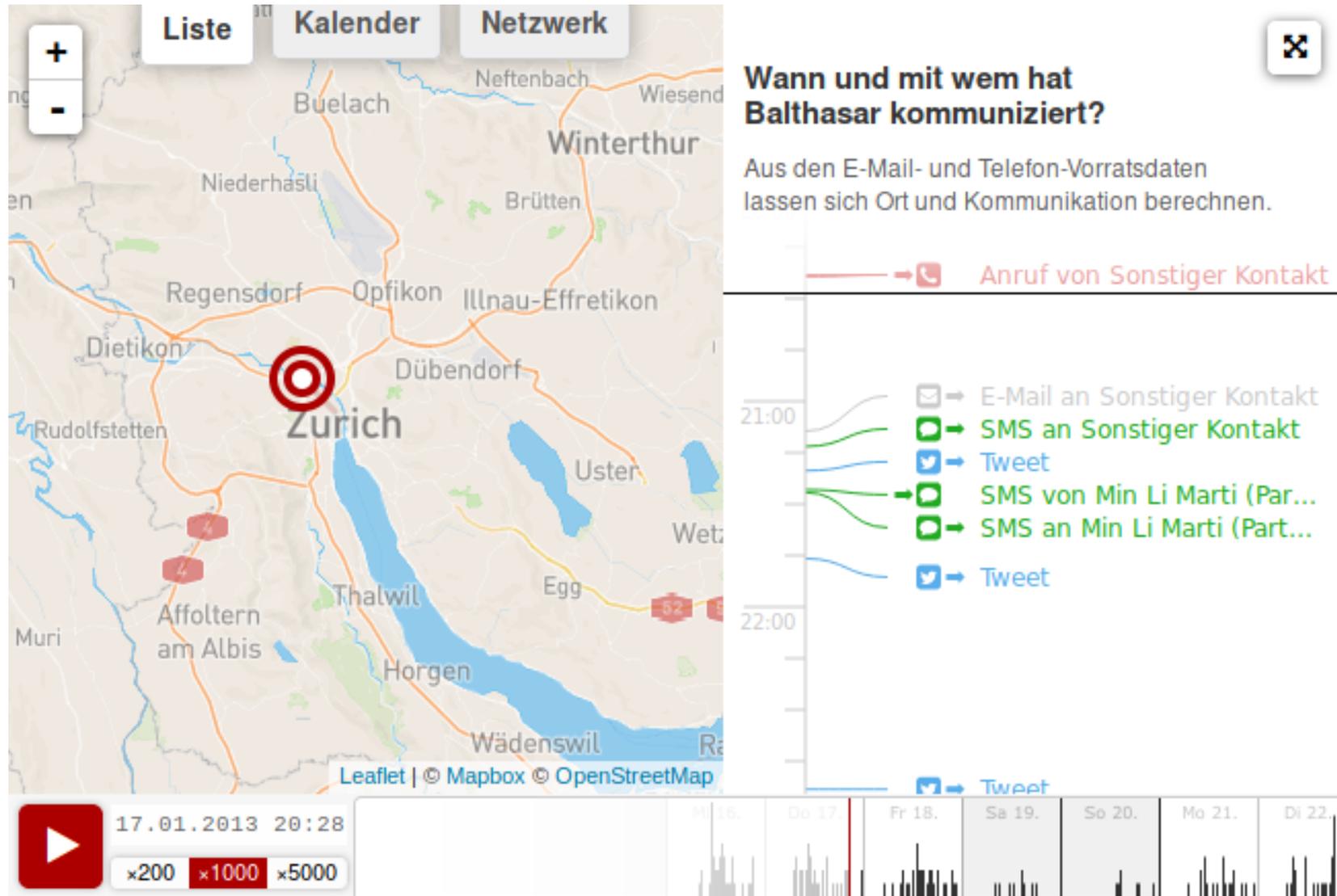


Bild von Selwyn van Haaren, unsplash.com

Über Metadaten

- ▶ Was sind Metadaten?
 - ▷ „Informationen über Informationen“
 - ▷ Beispiel SMS: u.a. Länge der Nachricht, Zeitpunkt, Ort (Funkzelle), Ursprung und Ziel
 - ▷ Metadaten verraten häufig mehr über Menschen als die eigentlichen Inhalte
- ▶ Für Geheimdienste besonders interessant
 - ▷ BND speicherte 2015 täglich 220 Millionen Metadaten

Verräterisches Telefon



Realisiert von [OpenDataCity](#). Über die Datenquelle: [digiges.ch](#). Anwendung steht unter [CC-BY 3.0](#).

Überwachung

- ▶ Geheimdienste werten Metadaten unter bestimmten Blickwinkeln aus ...

(Kontaktbeziehungen, Reisedaten, Finanztransfers, ...)

- ▶ ... bzw. setzen die gesammelten Daten gezielt ein

(z.B. in der Ukraine Anfang 2014. SMS an Teilnehmer einer Demonstration:

„Sehr geehrter Kunde, sie sind als Teilnehmer eines Aufruhrs registriert.“)

Smartphones: Hardware & Betriebssystem

- ▶ Hardware („Super-Wanze“)
 - ▷ Mikrofon, Kamera, GPS, Bewegungssensor...

- ▶ Betriebssystem: Goldener Käfig iOS (Apple)
 - ▷ Apps nur aus einer Quelle (zentraler App-Store)
 - ▷ geschlossenes System, keine Gerätehoheit
 - ▷ mehr Freiheit durch Jailbreak (Gefängnisausbruch)
 - ▷ massives Tracking durch Apps aus dem App-Store:
 - <https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/>

Android

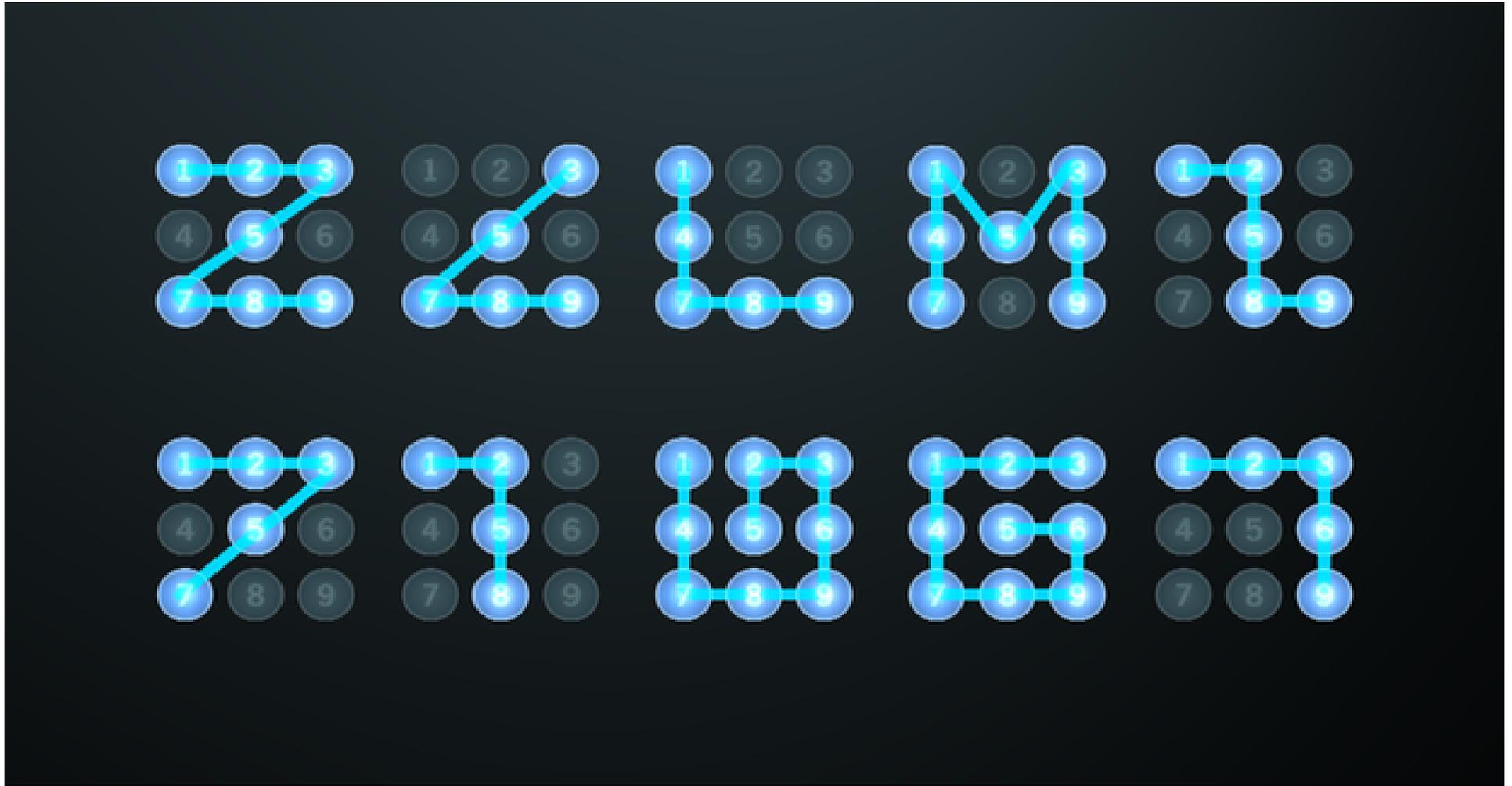
- ▶ Theoretisch gute Basis ...

- ▷ Linux-basiert, freie Software

- ▶ **Aber:**

- ▷ Google-Dienste bei Neugeräten fest integriert: Suche, Browser, Gmail, Maps, Kalender- / Kontakte-Sync ...
- ▷ Play Store & Google-Dienste
- ▷ Fernzugriff, Datenübermittlung
- ▷ standardmäßig keine Gerätehoheit
- ▷ oft unzureichende Versorgung mit Sicherheitsupdates durch den Hersteller, starke Abhängigkeit von Google

Typische Wischgesten



Erste Schritte: Konfiguration

- ▶ Sichere Bildschirmsperre
 - ▷ von unsicher zu sicher:
Wischgeste, Muster, Biometrisch, PIN, Passwort
- ▶ Gerätespeicher verschlüsseln
- ▶ WLAN, GPS, Bluetooth, etc. ausschalten, wenn nicht genutzt
- ▶ Browser (Firefox) gegen Tracking schützen (siehe 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

- ▶ Markt für optimierte personenbezogene Werbung
- ▶ Apps sammeln diverse Nutzerdaten (z. B. Standortdaten) und leiten diese weiter
- ▶ 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)



Lieferando

10 trackers

26 permissions

Version 6.7.0 - [see other versions](#)

Report created on Dec. 3, 2019, 8:46 p.m.

[See on Google Play >](#)

10 trackers

We have found **code signature** of the following trackers in the application:

[Ad4Screen >](#)

[Adjust >](#)

[Facebook Analytics >](#)

[Facebook Login >](#)

[Facebook Share >](#)

[Google Analytics >](#)

Apps immer kritisch begegnen!

- ▶ „Kostenlose“ Apps im App/Play Store verdienen häufig mit Datensammelei und Werbung an den Nutzer:innen
- ▶ Immer hinterfragen: Braucht App XY diese oder jene Berechtigung für ihre Funktion überhaupt?
- ▶ Einzelne Berechtigungen von Apps entziehen
- ▶ Auf Website ausweichen, wenn Dienst ohne App nutzbar ist.
- ▶ Alternative Apps nutzen, die weniger Berechtigungen benötigen

Android „entgoogeln“

- ▶ Apps und Dienste von Google deaktivieren/deinstallieren
 - ▷ Google-Einstellungen (G+, Standort, Suche, Werbe-ID, Assistant usw.)
- ▶ Alternativ-Dienste nutzen
 - ▷ Browser, Suche, Mail, Sync für Kalender / Kontakte ...
- ▶ Play Store deaktivieren / F-Droid nutzen
 - ▷ App-Alternativen nutzen
- ▶ Freie Android-Variante installieren
 - ▷ z.B. LineageOS, Replicant, /e/, OmniROM, GrapheneOS...

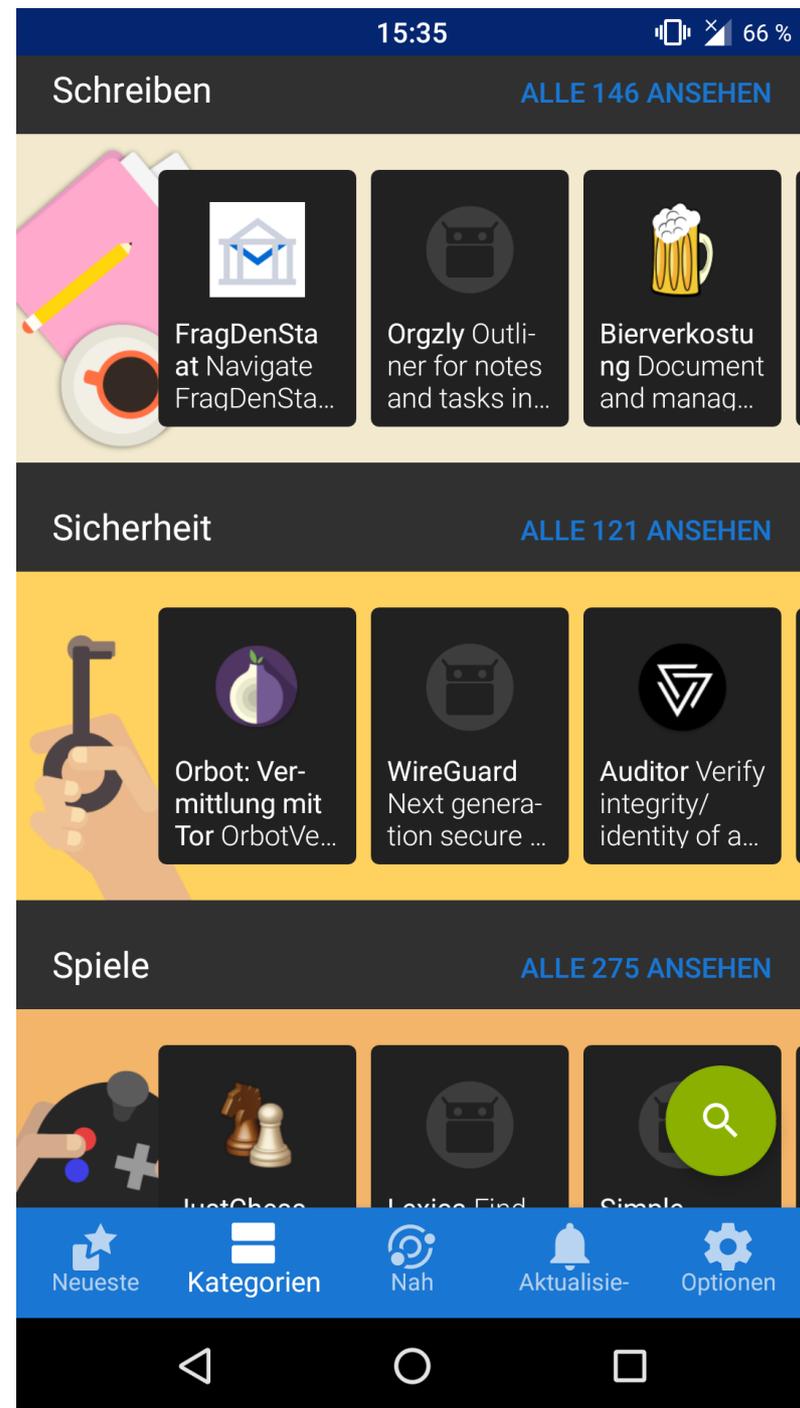
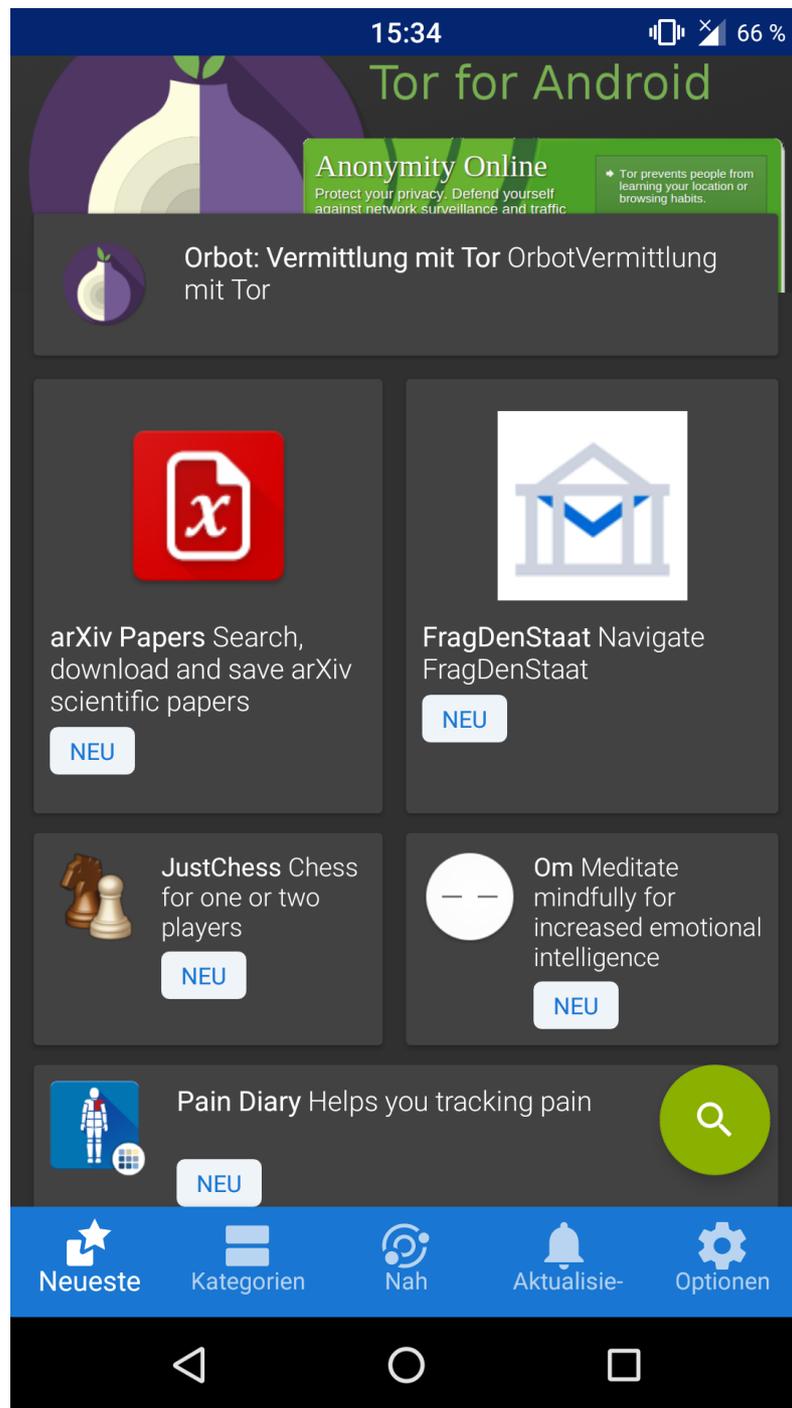
Empfehlenswerte Apps: F-Droid

- ▶ Alternative/Ergänzung zum Play Store: F-Droid
 - ▷ <https://f-droid.org/>
- ▶ Ausschließlich Software/Apps unter freier Lizenz
- ▶ Kein Nutzerkonto erforderlich
- ▶ Ergänzungen zum offiziellen F-Droid-Repository können von allen vorgeschlagen werden
- ▶ Es ist möglich, private Repositories zur Verfügung zu stellen und einzubinden
- ▶ Auch direkter Download von Apps über die Website möglich (dann keine automatischen Updates)



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)



Installation von F-Droid



<https://f-droid.org>

Ansprüche an Messenger

- ▶ für alle gängigen Betriebssysteme verfügbar
- ▶ Ende-zu-Ende-Verschlüsselung
- ▶ Sicherer Verschlüsselungsalgorithmus (AES)
- ▶ Dezentralität / Möglichkeit für eigene Server
- ▶ Quelloffen (Überprüfung durch unabhängige Experten)
- ▶ Upload von Daten (z.B. Adressbuch) nur mit ausdrücklicher Bestätigung des Nutzers
 - ▷ Adressbuch enthält Daten anderer Personen → Upload erlaubt?
- ▶ Unabhängige Installation und Betrieb
 - ▷ z.B. ohne Google Play Store & Google-Dienste

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/>

Empfehlenswerte Messenger

▶ **Conversations** (Android)



bzw. ChatSecure (iOS)

- ▶ nutzen das offene Protokoll **XMPP** (Jabber), das im Gegensatz zu anderen Messengern dezentrale Kommunikationsstrukturen erlaubt
 - ▶ unterstützen Ende-zu-Ende-verschlüsselte Chats via OMEMO
 - ▶ verfügbar via F-Droid (Conversations) bzw. App Store (ChatSecure)
 - ▶ als Conversations Legacy auch kostenlos im Play Store
- ▶ **Weitere Alternativen:**
- ▶ Android: Pix-Art Messenger
 - ▶ IOS: Monal, Siskin IM

Empfehlenswerte Browser



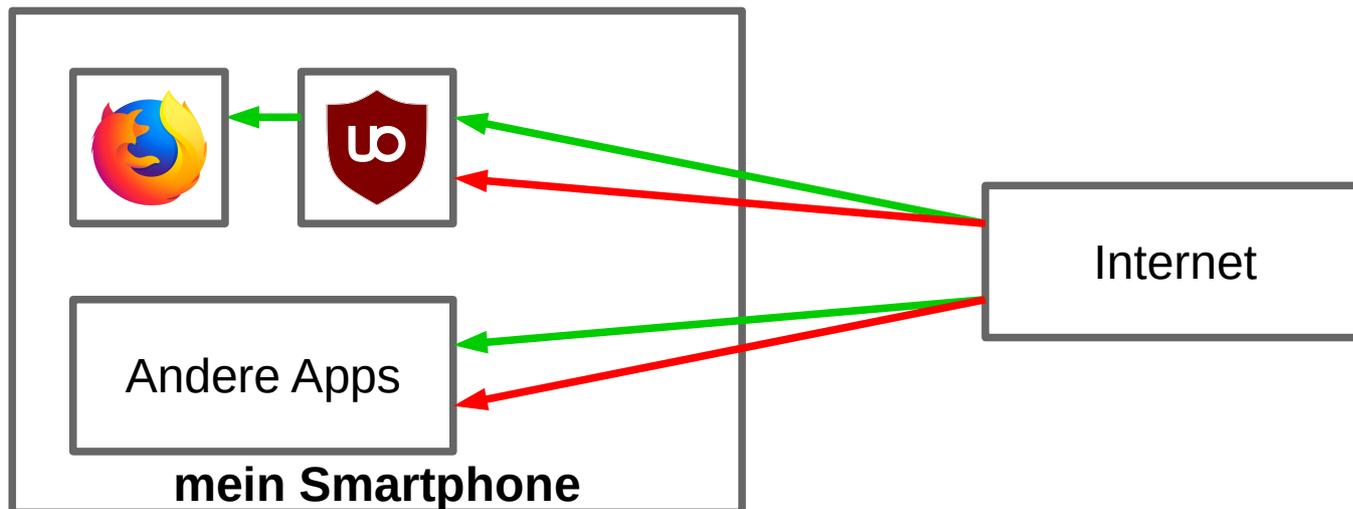
▶ Mozilla Firefox / Fennec F-Droid

- ▷ Freie Software
- ▷ unter Android durch Add-ons erweiterbar (uBlock Origin, NoScript, HTTPS Everywhere etc.)
- ▷ Konfiguration ähnlich zur Desktop-Version
- ▷ iOS-Version stark eingeschränkt

▶ Tor Browser ebenfalls für Android verfügbar

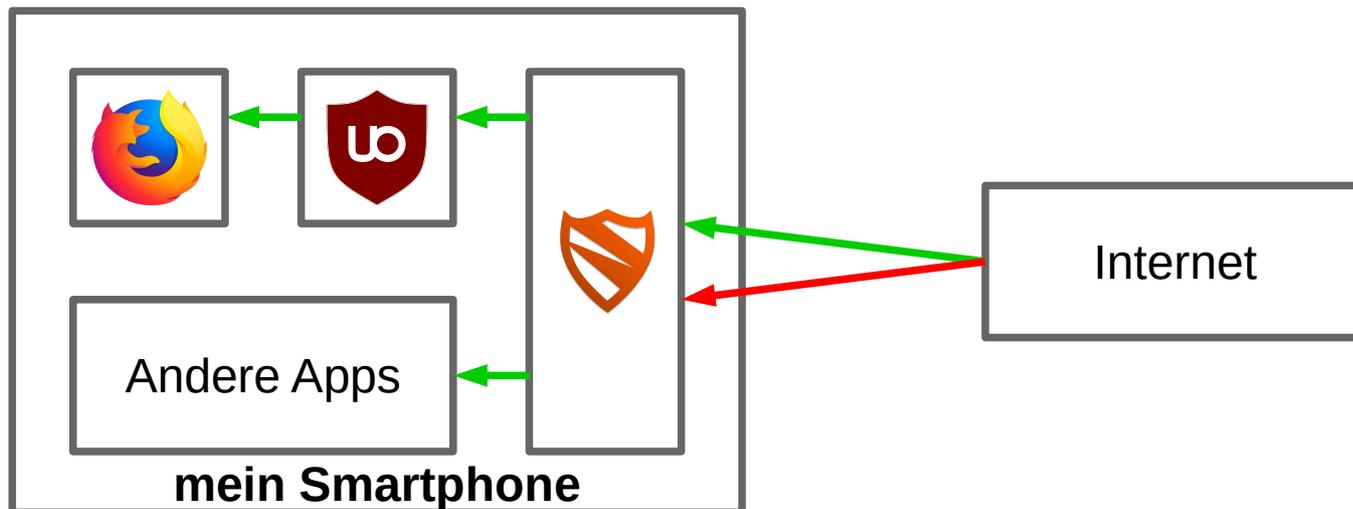
Werbung auf Systemebene blockieren

- ▶ Adblocker ▶ wirkt nur im Browser
- ▶ Weiterhin Werbung in anderen Apps



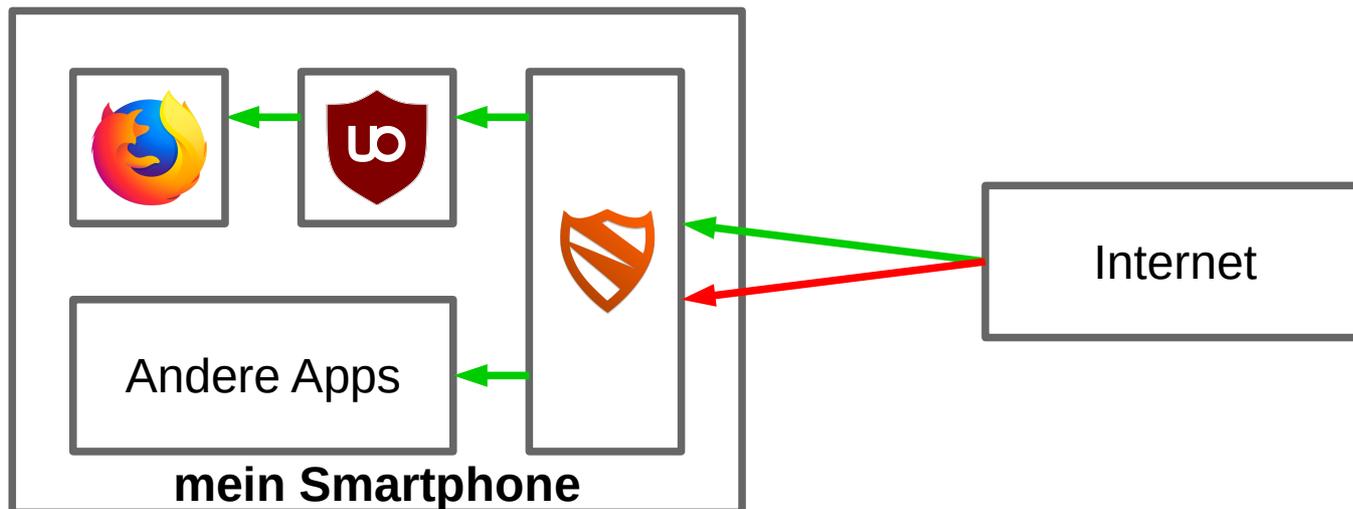
Werbung auf Systemebene blockieren

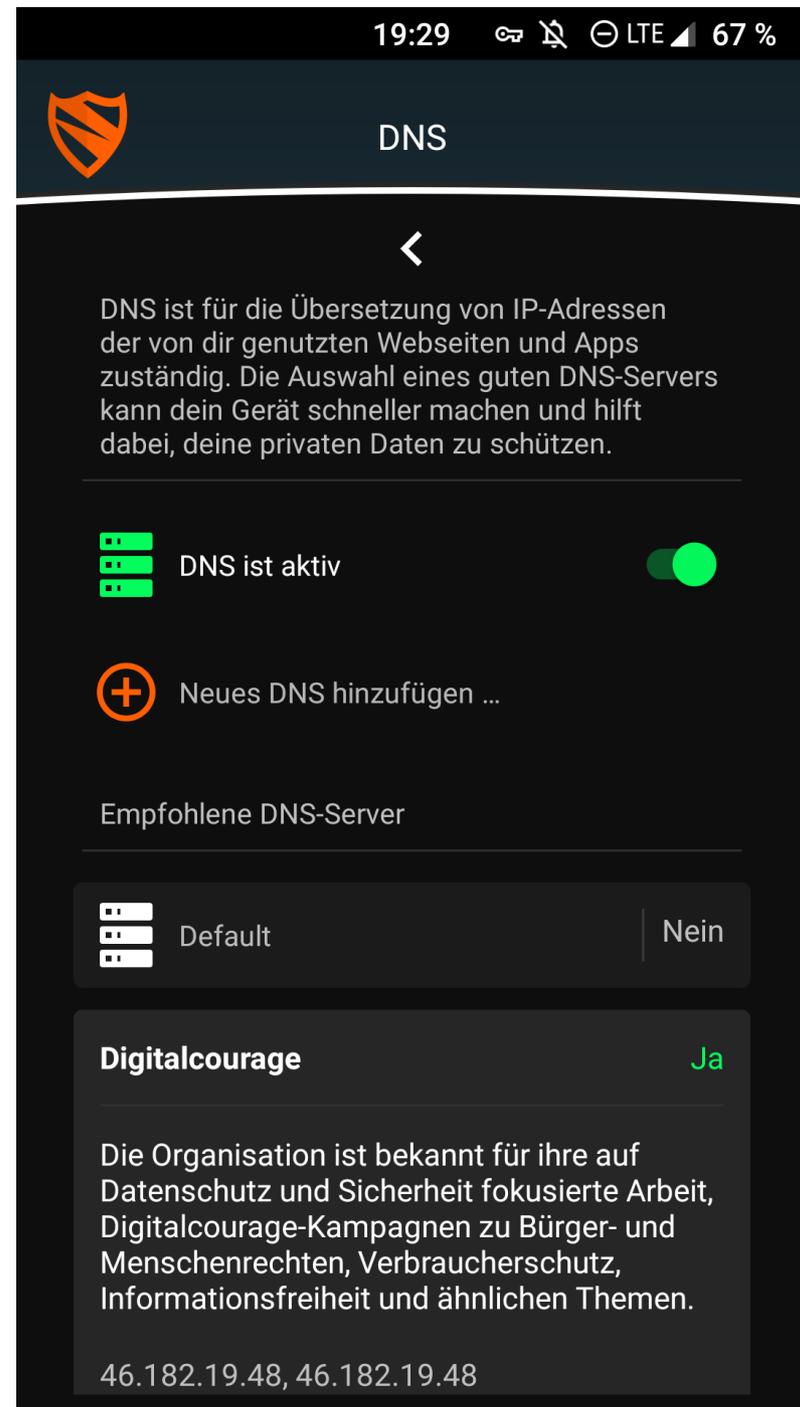
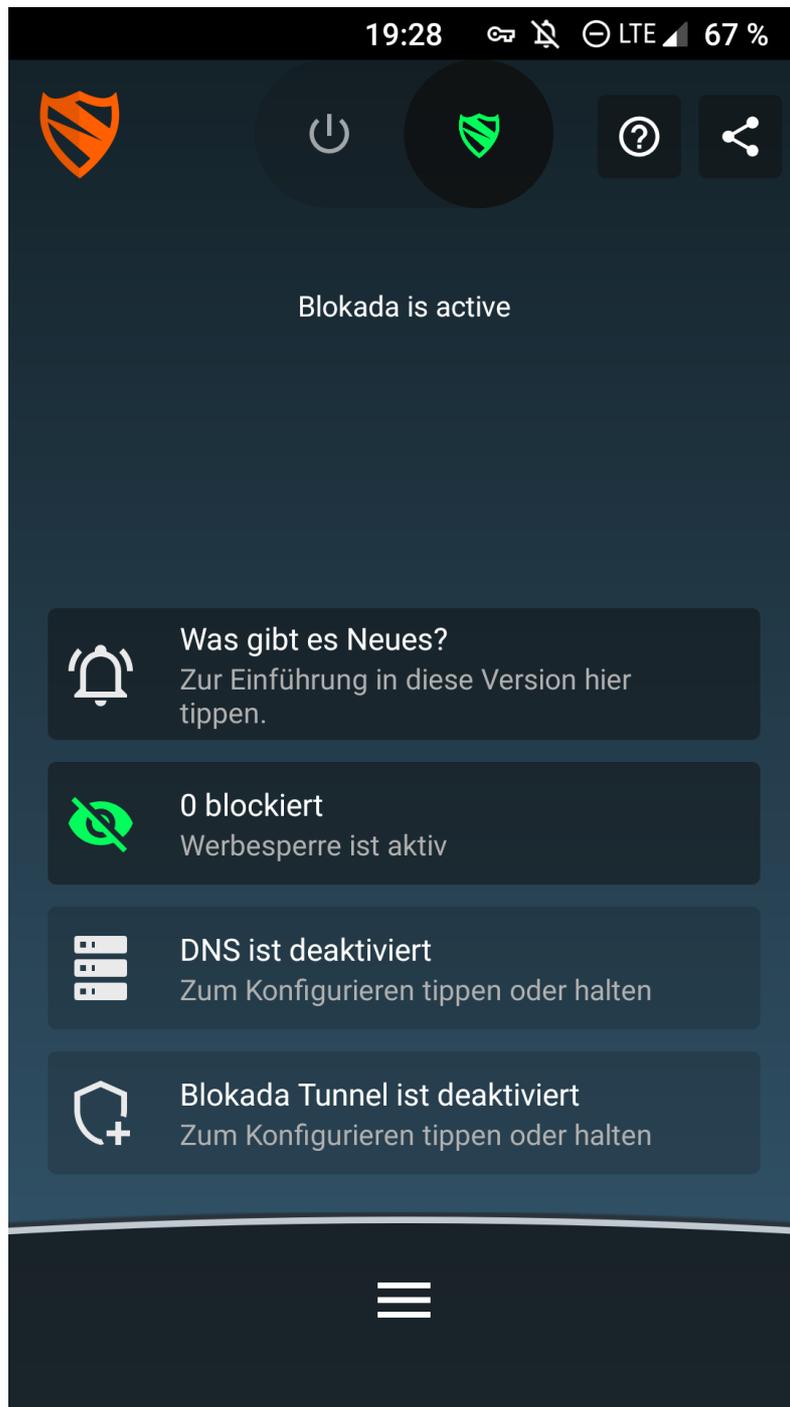
- ▶ Sämtliche Daten laufen über Blokada
- ▶ Nicht mit anderen Diensten kompatibel, die die VPN-Schnittstelle nutzen (z.B. Tor, OpenVPN, NetGuard)



Werbung auf Systemebene blockieren

- ▶ Funktioniert nur bei Android, Installation über F-Droid oder als APK unter <https://blokada.org/#download>
 - ▷ Auch für iOS verfügbar, aber nicht quelloffen (?)





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 kloniert Apps ins Arbeitsprofil
 - "Böse" Apps vom Rest des Systems isolieren
 - Apps mit verschiedenen Accounts nutzen



Empfehlenswerter E-Mail-Client

▶ K-9 Mail



- ▷ Umfangreicher, freier Mail-Client
- ▷ Unterstützt IMAP/POP3
- ▷ Kann verschlüsselte Mails via PGP/MIME senden und empfangen

▶ OpenKeychain



- ▷ Implementierung von OpenPGP unter Android
- ▷ Agiert außerdem als Schlüsselverwaltung
- ▷ Problem: private Schlüssel auf Mobilgerät zu gefährdet?

Weitere empfehlenswerte Apps



▶ **Transportr**

- ▷ Fahrpläne des öffentlichen Nah-/Fernverkehrs & Verbindungssuche



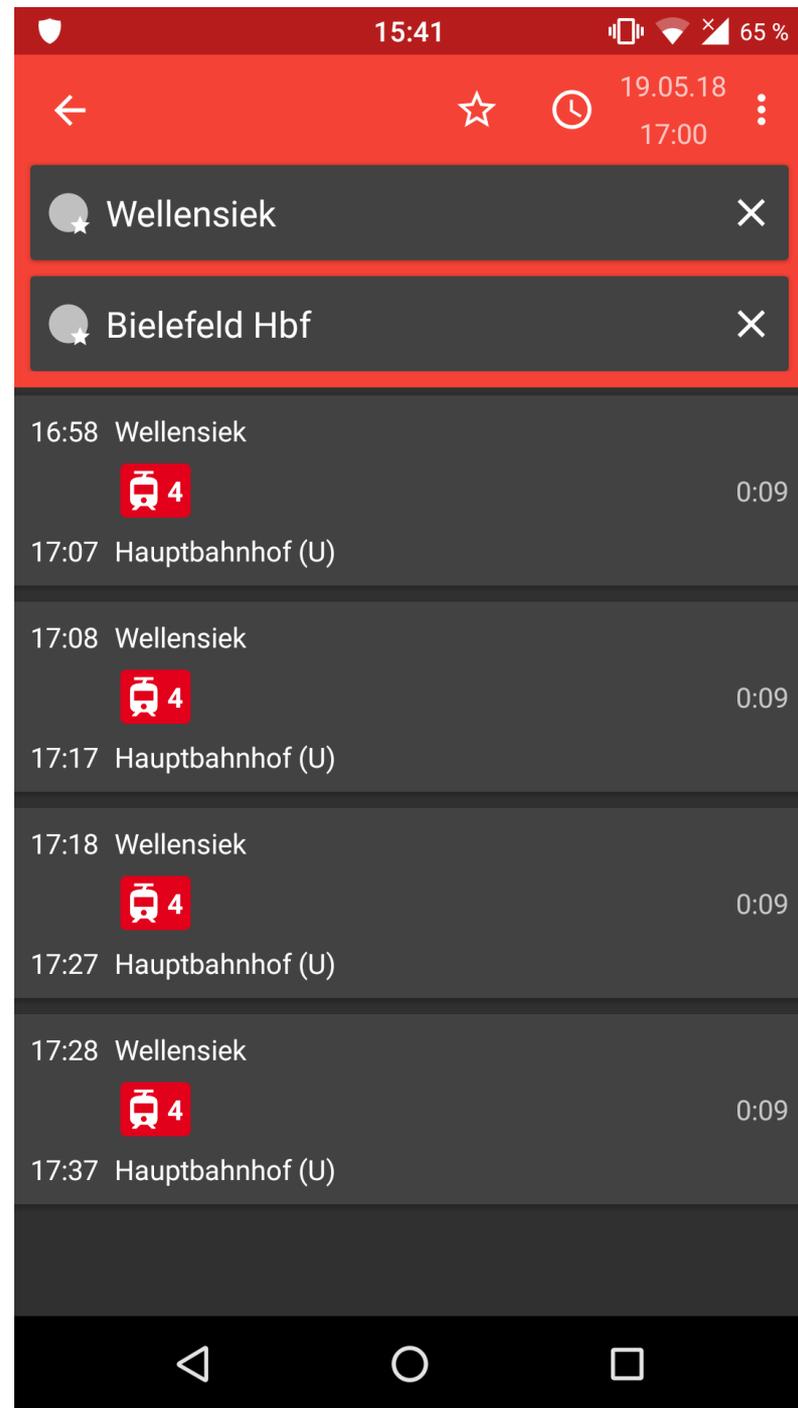
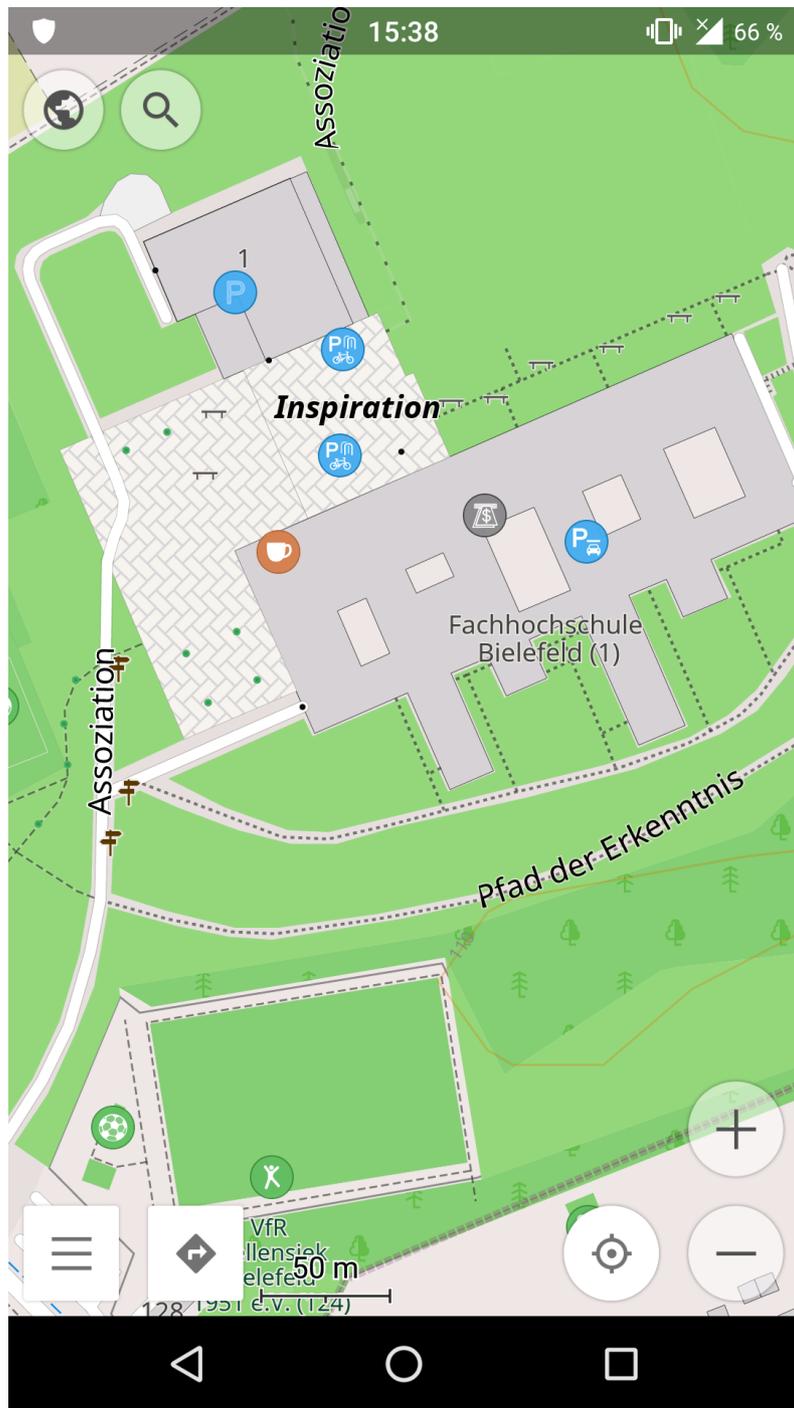
▶ **VLC**

- ▷ Video- und Audioplayer



▶ **OsmAnd+**

- ▷ Karten- und Navigationssoftware auf Basis von OpenStreetMap, unterstützt auch Offline-Karten



... und was ist mit iOS?

- ▶ Einige App-Empfehlungen:
 - ▷ **Blokada:** Werbung und Tracking via VPN-Schnittstelle systemweit unterbinden.
 - ▷ **Collabora Office:** Office-Suite auf Basis von LibreOffice.
 - ▷ **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.
 - ▷ **VLC for Mobile:** Bekannter Video- und Audioplayer, der mit vielen Formaten umgehen kann.

Zur Corona-Warn-App des RKI ...

- ▶ „Wie hältst du's mit der Corona-Warn-App?“
Eine moderne Gretchenfrage

<https://digitalcourage.de/blog/2020/corona-warn-app-gretchenfrage>

- ▶ Wägt selbst ab, ob ihr die App verwenden wollt.

Links & Literatur

▶ **PRISM Break zu Android & iOS**

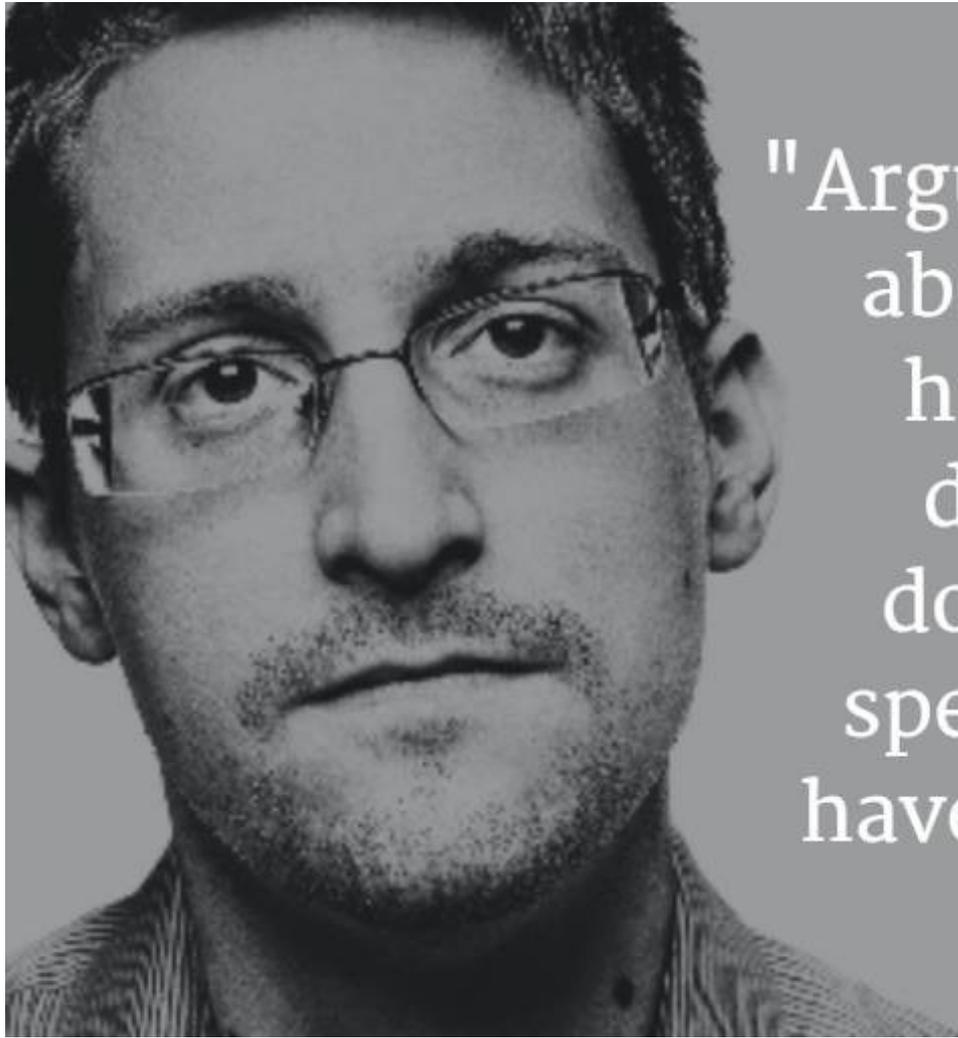
- ▷ <https://prism-break.org/de/categories/android/>
- ▷ <https://prism-break.org/de/categories/ios/>

▶ **Artikelreihen zu Android von Mike Kuketz**

- ▷ <https://www.kuketz-blog.de/android-ohne-google-take-back-control-teil1/>
- ▷ <https://www.kuketz-blog.de/your-phone-your-data-light-android-unter-kontrolle/>

▶ **Digitalcourage: Digitale Selbstverteidigung**

- ▷ <https://digitalcourage.de/digitale-selbstverteidigung/mobil>



"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."

– Ende –