Smartphones datenschutzfreundlich nutzen

digitalcourage Hochschulgruppe

Jan

Digitalcourage e.V.

- Gemeinnütziger Verein für Datenschutz und Bürgerrechte
  - "Für eine lebenswerte Welt im digitalen Zeitalter"
  - Big Brother Awards
  - Aktionen zu aktuellen Themen

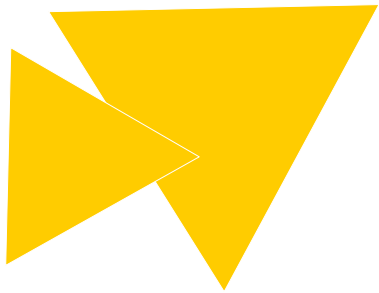
- Digitalcourage-Hochschulgruppe ***(www.digitalcourage.de/hsg)***
  - CryptoPartys → 21. November
  - Backup-Partys → 28. November
  - Linux-Install-Partys → 6. Dezember
  - Regelmäßige Treffen an der Uni → 1.+3. Montag im Monat

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



Überwachung

- Geheimdienste werten Metadaten unter bestimmten Blickwinkeln aus...

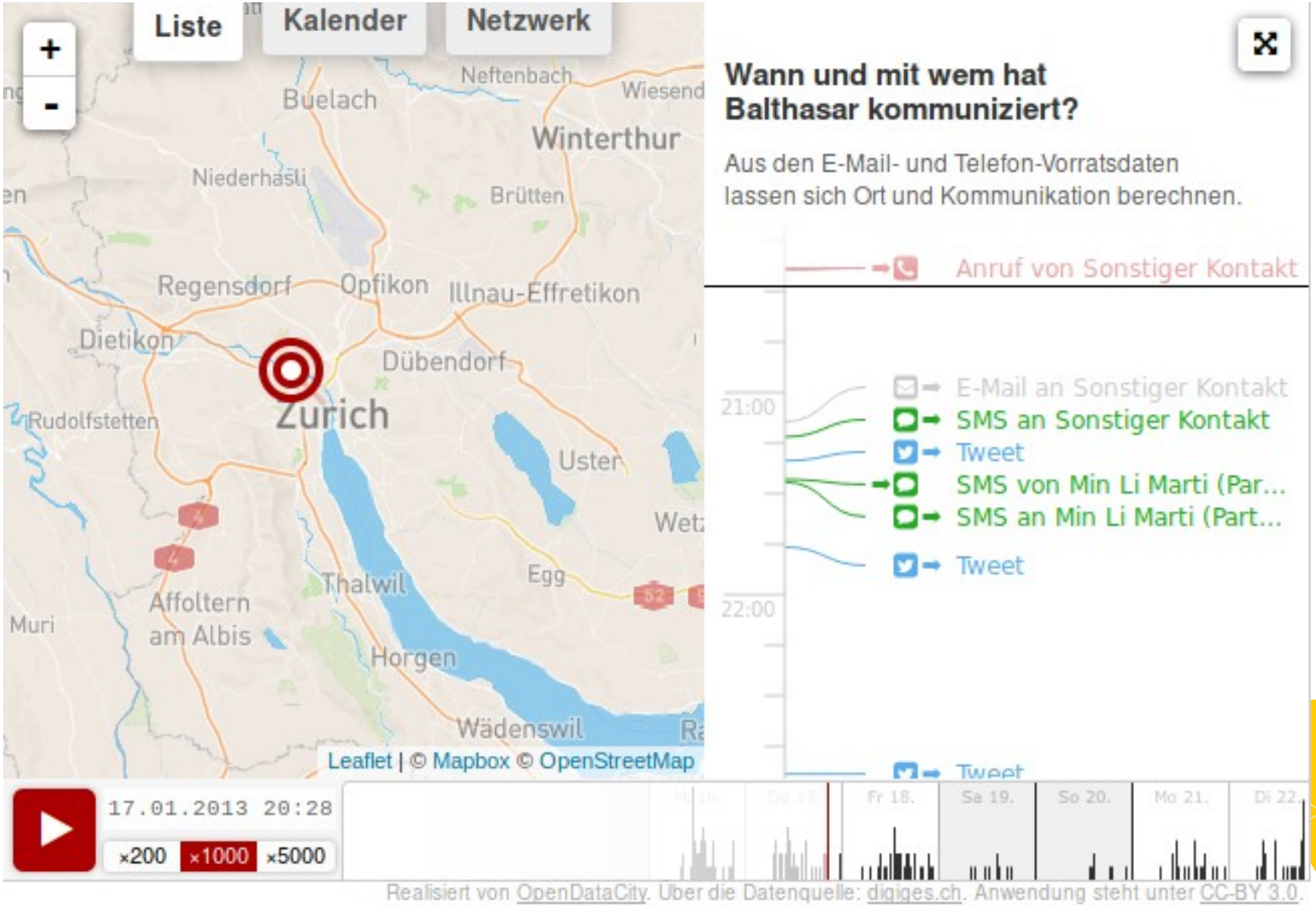
  (Kontaktbeziehungen, Reisedaten, Finanztransfers, ...)

- ...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.")

Verräterisches Smartphone



Kommerzielle Datensammlungen

- Neuer 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)

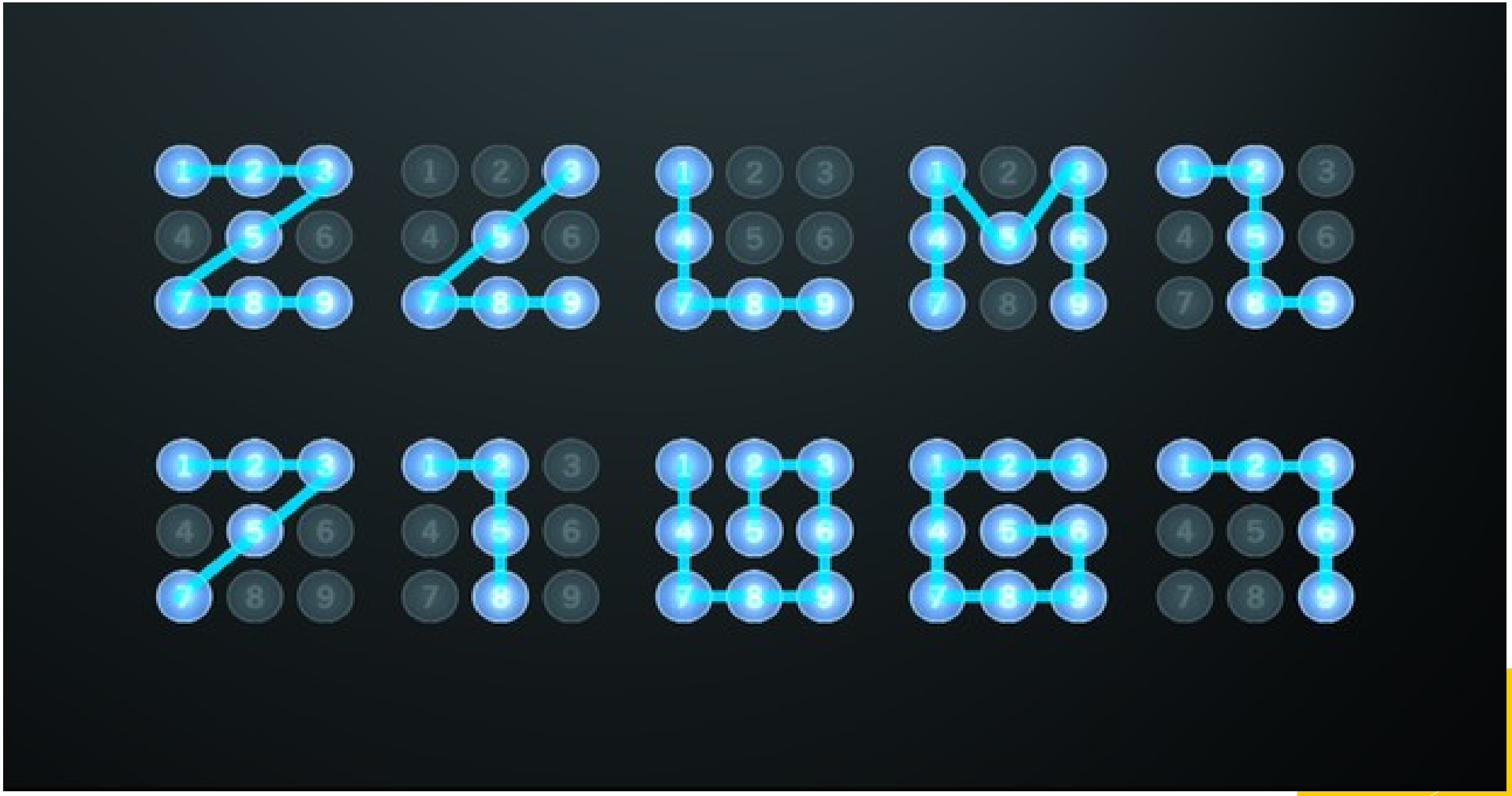
Smartphones: Hardware & Betriebssystem

- 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)

Android

- Theoretisch gute Basis...
  - Linux-basiert, freie Software
- **Aber:** tiefe Integration proprietärer Google-Software
  - Suche, Browser, Gmail, Maps, Kalender- / Kontakte-Sync …
  - Play Store & Google-Dienste
  - Fernzugriff, Datenübermittlung
  - Standardmäßig keine Gerätehoheit
  - Oft unzureichende Versorgung mit Sicherheitsupdates durch den Hersteller

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

Super sichere Iris-Scanner?

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)

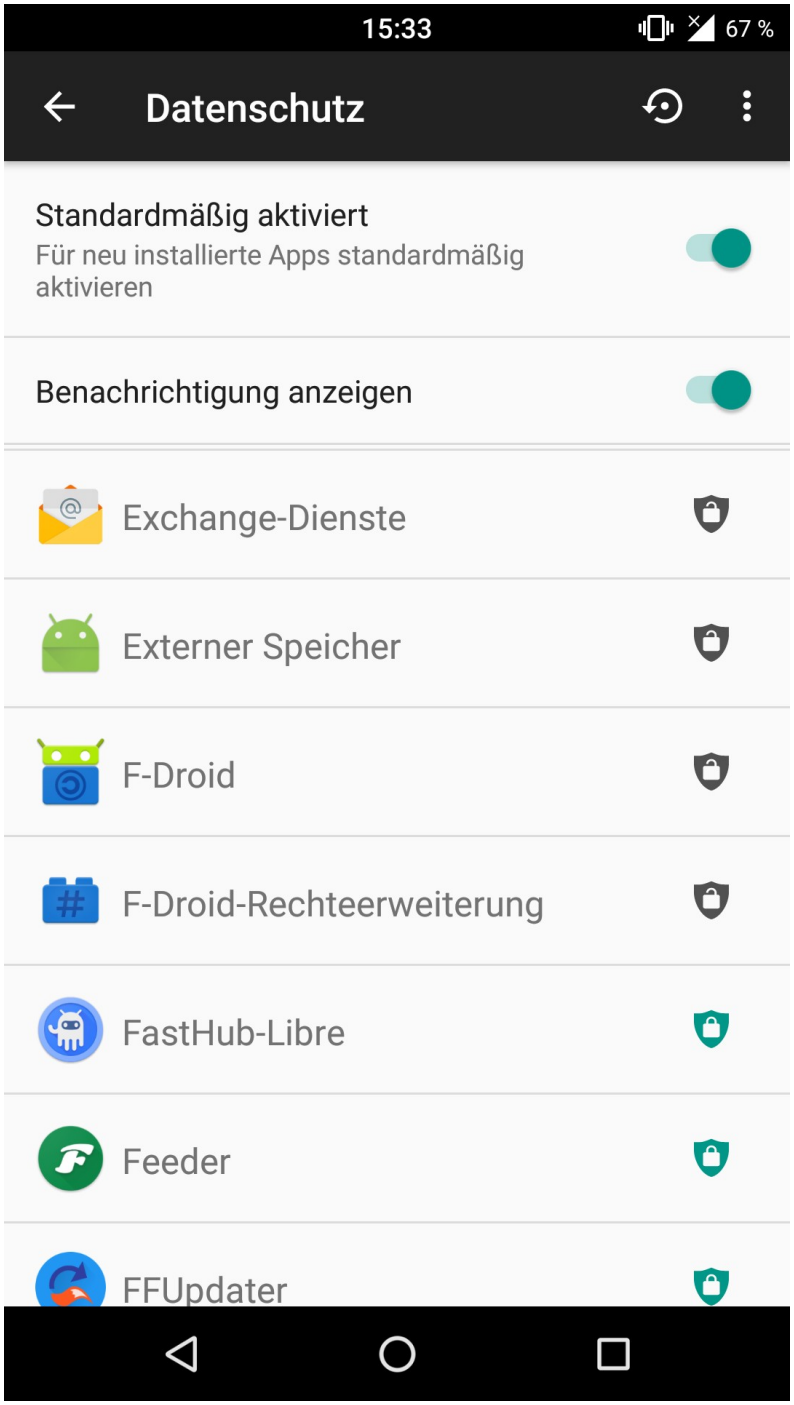
- Kamera
  - Bilder und Videos aufzeichnen
- Mikrofon
  - Ton aufzeichnen
- WLAN-Verbindungsinformationen
  - WLAN-Verbindungen abrufen
- Geräte-ID & Anrufinformationen
  - Telefonstatus und Identität

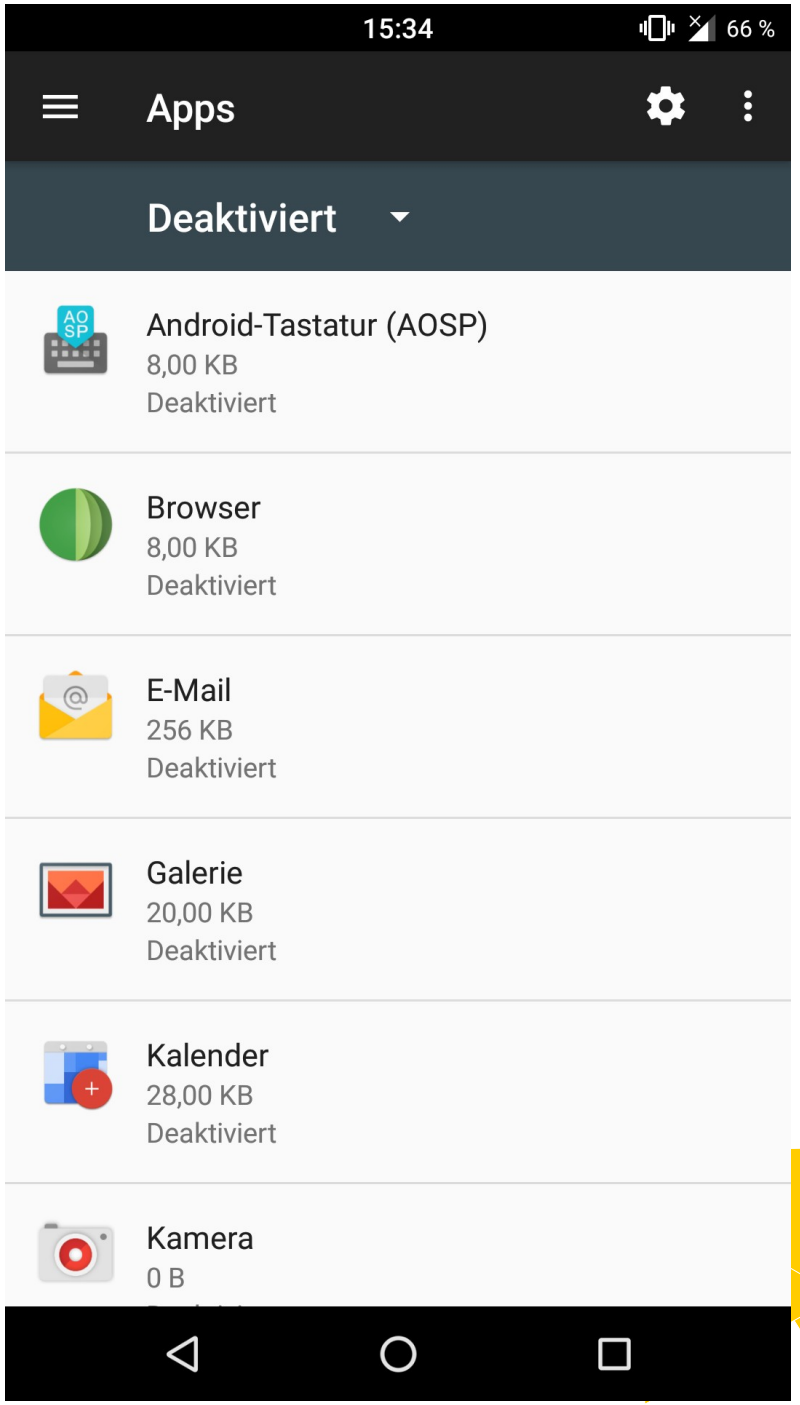
App-Berechtigungen: Facebook (4)

- 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

App-Berechtigungen

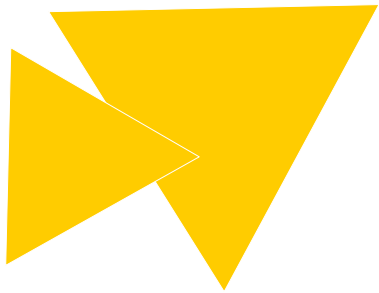
- „Kostenlose“ Apps im App/Play Store verdienen häufig mit Datensammelei und Werbung an den Nutzer.innen
- Apps immer kritisch hinterfragen: Braucht App XY diese oder jene Berechtigung für ihre Funktion überhaupt?
- Einzelne Berechtigungen von Apps entziehen.
- Falls verfügbar: Datenschutzmodus aktivieren!
- Alternative Apps nutzen, die weniger Berechtigungen benötigen.


15:33
67 %
Datenschutz
Standardmäßig aktiviert
Für neu installierte Apps standardmäßig aktivieren
Benachrichtigung anzeigen
Exchange-Dienste
Externer Speicher
F-Droid
F-Droid-Rechteerweiterung
FastHub-Libre
Feeder
FFUpdater


15:34
66 %
Apps
Deaktiviert
Android-Tastatur (AOSP)
8,00 KB
Deaktiviert
Browser
8,00 KB
Deaktiviert
E-Mail
256 KB
Deaktiviert
Galerie
20,00 KB
Deaktiviert
Kalender
28,00 KB
Deaktiviert
Kamera
0 B

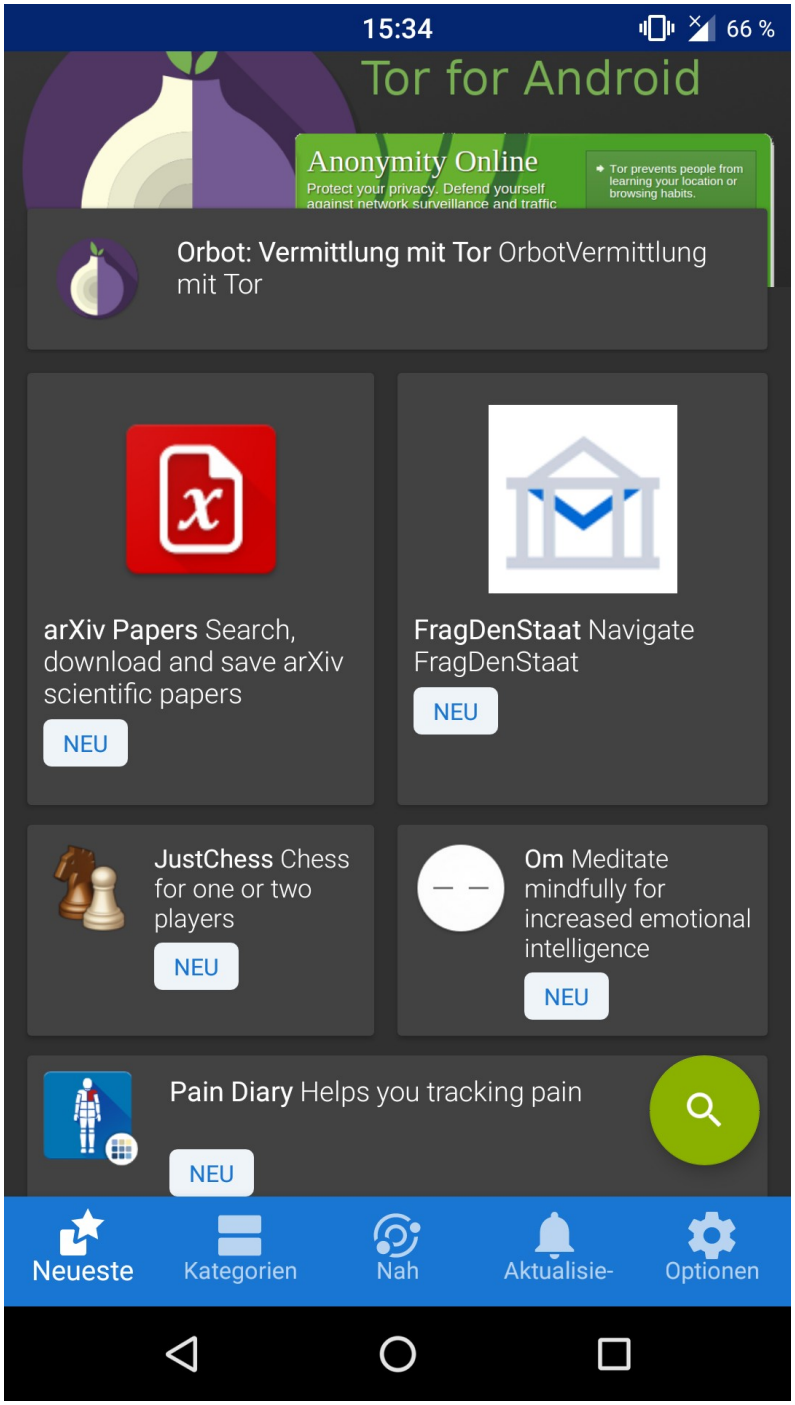
Android „entgoogeln“

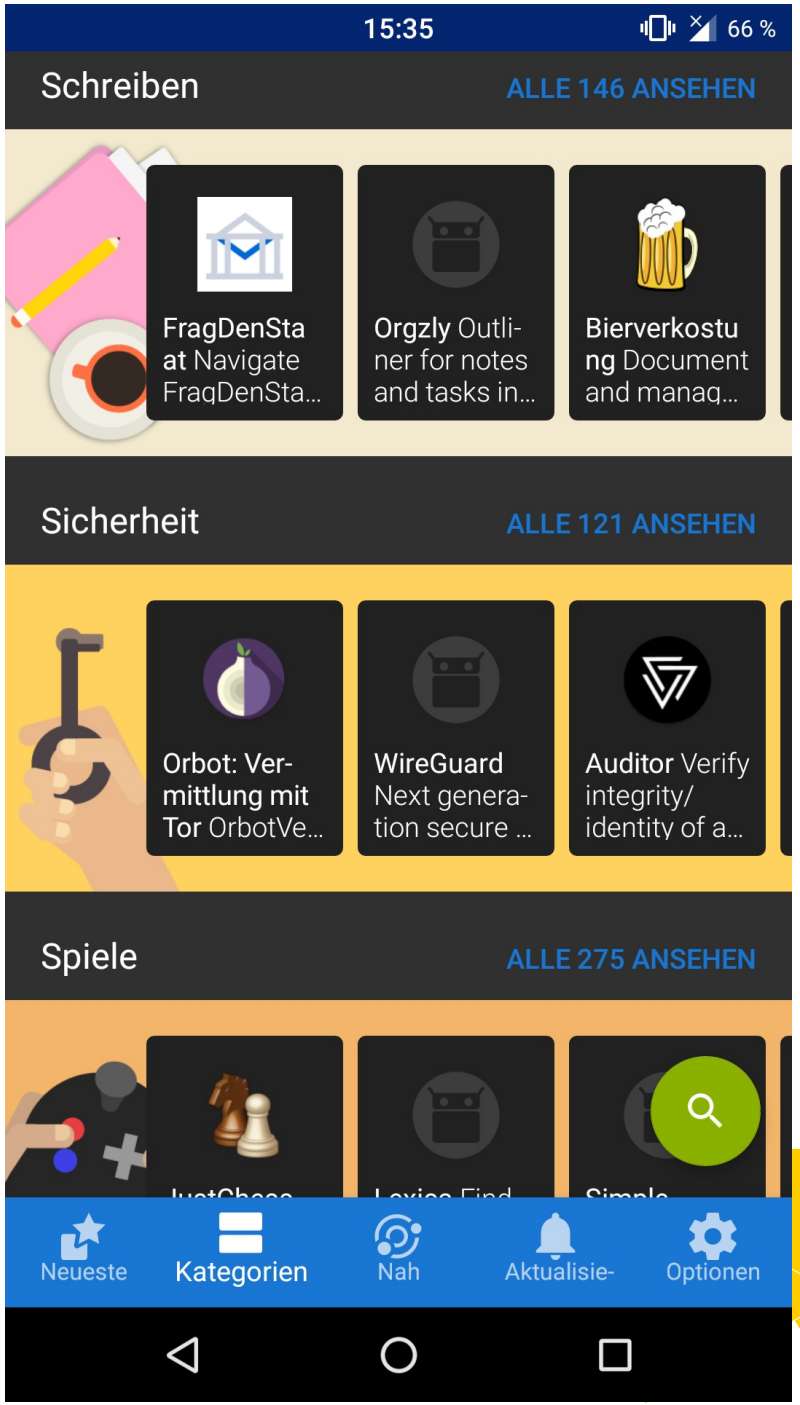
1. Apps und Dienste von Google deaktivieren/deinstallieren
   - Google-Einstellungen (G+, Standort, Suche, Werbe-ID, usw.)
2. Alternativ-Dienste nutzen
   - Browser, Suche, Mail, Sync für Kalender / Kontakte...
3. Play Store deaktivieren / F-Droid nutzen
   - App-Alternativen nutzen
4. Freie Android-Variante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



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)


15:34
66 %
Tor for Android
Anonymity Online
Protect your privacy. Defend yourself against network surveillance and traffic
Tor prevents people from learning your location or browsing habits.
Orbot: Vermittlung mit Tor OrbotVermittlung mit Tor
arXiv Papers Search, download and save arXiv scientific papers
NEU
FragDenStaat Navigate FragDenStaat
NEU
JustChess Chess for one or two players
NEU
Om Meditate mindfully for increased emotional intelligence
NEU
Pain Diary Helps you tracking pain
NEU
Neueste
Kategorien
Nah
Aktualisie-
Optionen


15:35
66 %
Schreiben
ALLE 146 ANSEHEN
FragDenSta at Navigate FragDenSta...
Orgzly Outli- ner for notes and tasks in...
Bierverkostu ng Document and manag...
Sicherheit
ALLE 121 ANSEHEN
Orbot: Ver- mittlung mit Tor OrbotVe...
WireGuard Next genera- tion secure ...
Auditor Verify integrity/ identity of a...
Spiele
ALLE 275 ANSEHEN
Neueste
Kategorien
Nah
Aktualisie-
Optionen

Ansprüche an Messenger

- Für alle gängigen Betriebsysteme 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

Messenger-Vergleich (Android

	Signal	Telegram	Briar	Threema	WhatsApp
Freie Software	ja	teils	ja	nein	nein
Ende-zu-Ende-Verschlüsselung	ja	(ja)	ja	(ja)	(ja)
unabhängiges Audit	ja	ja	ja	(ja)	nein
Adressbuch-Zugriff	ja	ja	nein	(nein)	(nein)
Nicknames (Pseudonyme)	nein	nein	ja	ja	nein
außerhalb Play-Store erhältlich	ja	ja	ja	ja	ja
funktioniert ohne Google-Dienste	ja	ja	ja	ja	nein
Verbreitung	mittel	weit	sehr gering	mittel	sehr weit

Alternative zu WhatsApp & Co

- **Signal** (Android, iOS)

  - Freie Software
  - Sicherer Verschlüsselungsalgorythmus
  - Unterstützt verschlüsselte Text- und Sprachnachrichten, Telefonie und SMS.
  - Telefonnummer zwingend erforderlich, zentrale Struktur
  - Kostenlos im Play bzw. App Store, für Android auch als APK:
    - https://signal.org/android/apk/

Empfehlenswerte Messenger

- **Conversations (Legacy)** (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 OpenPGP, OTR und OMEMO
  - Verfügbar via F-Droid (Conversations) bzw. App Store (ChatSecure)
  - Als Conversations Legacy auch kostenlos im Play Store

Empfehlenswerter 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

Empfehlenswerter E-Mail-Client

- **K-9 Mail**
  - umfangreicher, freier Mail-Client
  - unterstützt IMAP/POP3
  - kann verschlüsselte Mails via PGP/MIME senden und empfangen

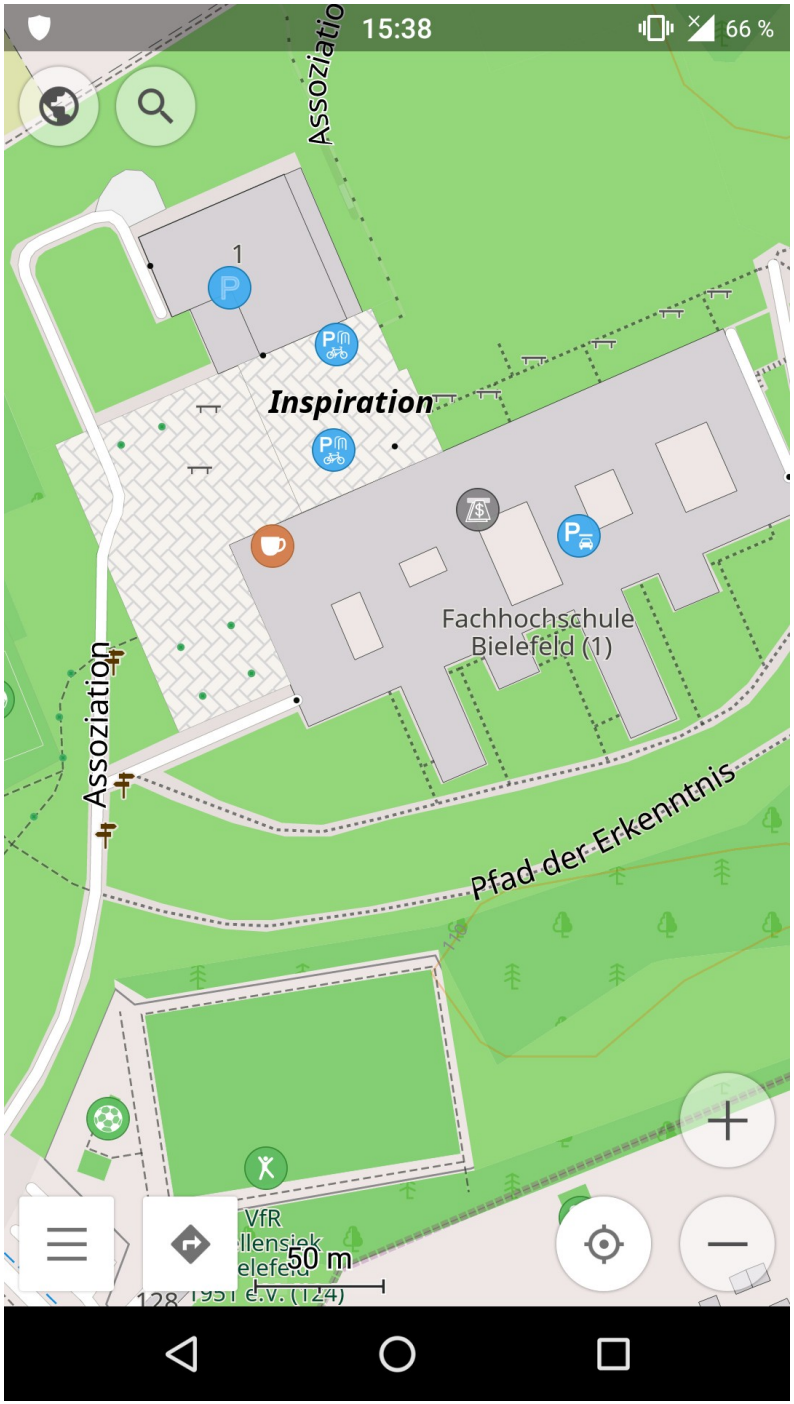
- **OpenKeychain**
  - Implementierung von OpenPGP unter Android
  - agiert außerdem als Schlüsselverwaltung
  - Problem: private Schlüssel auf Mobilgerät zu gefährdet?

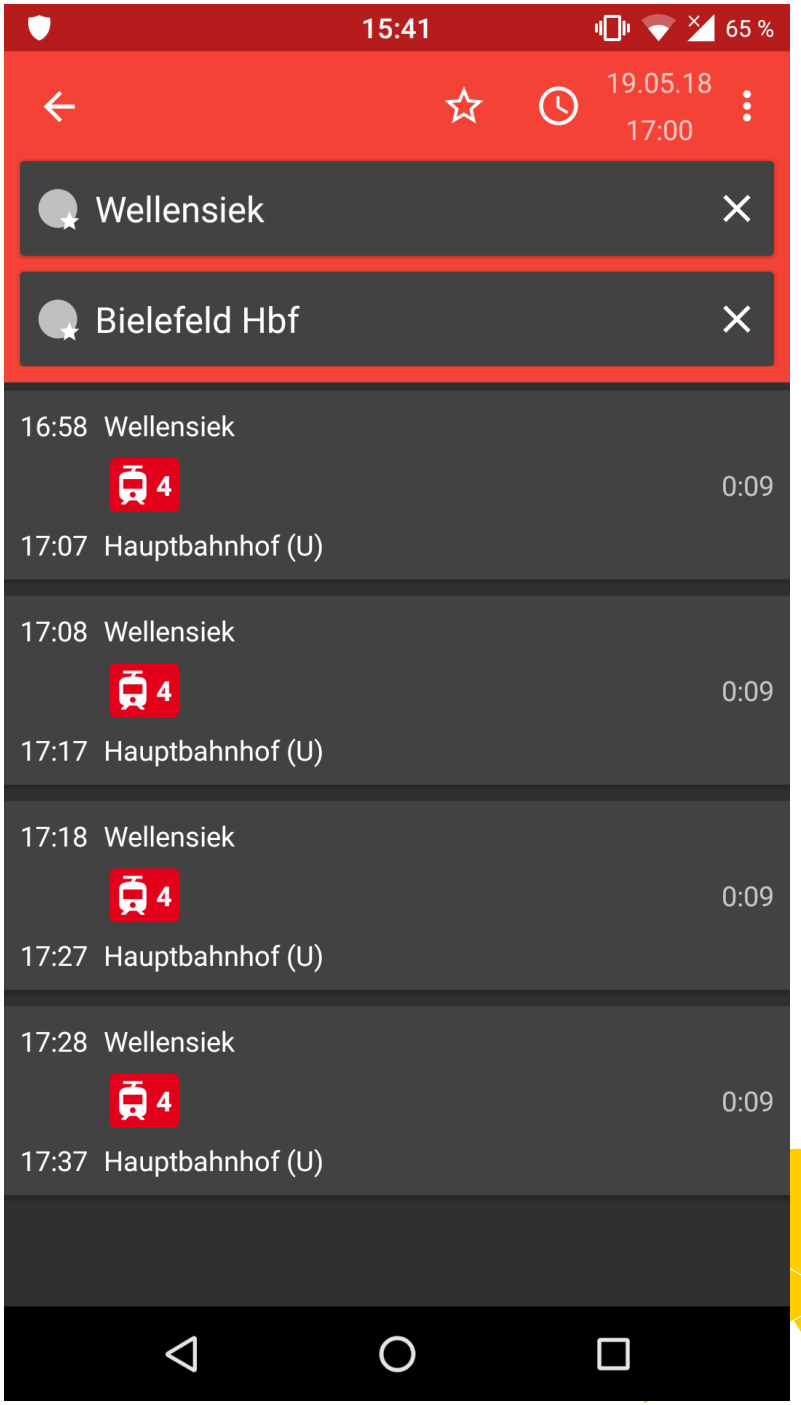
Weitere empfehlenswerte Apps

- **Transportr**
  - Fahrpläne des öffentlichen Nahverkehrs & Verbindungssuche

- **VLC**
  - Video- und Audioplaye

- **OsmAnd+**
  - Karten- und Navigationssoftware auf Basis von OpenStreetMap
  - unterstützt auch Offline-Karten


15:38
66 %
Assoziatio
1
Inspiration
Fachhochschule
Bielefeld (1)
Assoziation
Pfad der Erkenntnis
50 m


15:41
65 %
19.05.18
17:00
Wellensiek
Bielefeld Hbf
16:58 Wellensiek
4
0:09
17:07 Hauptbahnhof (U)
17:08 Wellensiek
4
0:09
17:17 Hauptbahnhof (U)
17:18 Wellensiek
4
0:09
17:27 Hauptbahnhof (U)
17:28 Wellensiek
4
0:09
17:37 Hauptbahnhof (U)

Links & Literatur

- **PRISM Break zu Android & iOS**
  - https://prism-break.org/de/categories/android/
  - https://prism-break.org/de/categories/ios/
- **Mike Kuketz: Your Phone Your Data (light) – Android unter Kontrolle**
  - https://www.kuketz-blog.de/your-phone-your-data-light-android-unter-kontrolle/
- **Digitalcourage: Digitale Selbstverteidigung**
  - https://digitalcourage.de/digitale-selbstverteidigung/mobil

Weitere Projekte

- **PRISM Break:** (https://prism-break.org/de/all/)
  Liste datenschutzfreundlicher Software und Anbieter
- **Digitalcourage: Digitale Selbstverteidigung**
  (https://digitalcourage.de/digitale-selbstverteidigung)
  - Übersichts-Flyer hier im Raum zum Mitnehmen!
- **CryptoPartys weltweit!**
  - https://www.cryptoparty.in/ (auf Englisch)
- **Freifunk Bielefeld**
  - https://www.freifunk-bielefeld.de/

Weitere Projekte

- **PRISM Break:** (https://prism-break.org/de/all/)
  Liste datenschutzfreundlicher Software und Anbieter
- **Digitalcourage: Digitale Selbstverteidigung**
  (https://digitalcourage.de/digitale-selbstverteidigung)
  - Übersichts-Flyer hier im Raum zum Mitnehmen!
- **CryptoPartys weltweit!**
  - https://www.cryptoparty.in/ (auf Englisch)
- **Freifunk Bielefeld**
  - https://www.freifunk-bielefeld.de/

Anlaufstellen & Projekte in Göttingen

- **CCC Göttingen**
  - Öffentliches Treffen (OpenChaos) jeden zweiten Dienstag um 20 Uhr im Hackerspace Neotopia an der Von-Bar-Straße 2-4 ("MLP-Haus").
  - https://cccgoe.de/

- **Freifunk Göttingen**
  - https://freifunk-goettingen.de/

Vielen Dank fürs Mitmachen!

(Bild: CC-BY-2.0: EFF)