

Crypto Course Magdeburg

23. November 2019



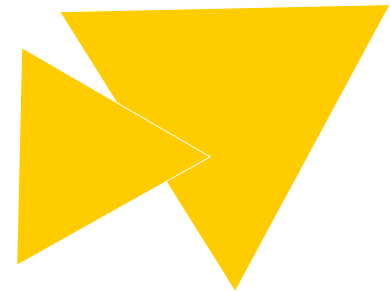
Jan & Julia



Digitalcourage e.V.

- ▶ non-profit association for data protection and civil rights
 - ▷ "for a world worth living in the digital age"
 - ▷ Big Brother Awards
 - ▷ Actions on current topics

- ▶ Digitalcourage university group Bielefeld (www.digitalcourage.de/hsg-bi)
 - ▷ CryptoParties, Backup Parties, Linux Install Parties
 - ▷ Regular meetings at the university

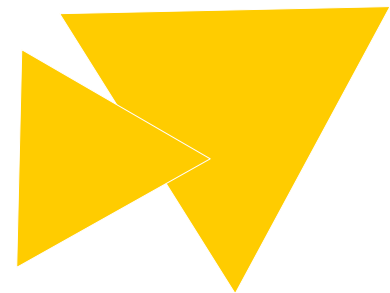


CryptoParty

- ▶ Digital self-defense
- ▶ Protection against mass surveillance
- ▶ Beginner friendly
- ▶ Public, non-commercial, worldwide
- ▶ By users for users
- ▶ Join in and become part of the CryptoParty movement

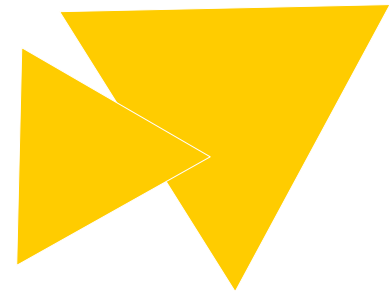
▶ <https://cryptoparty.in>

CRYPTO
PARTY

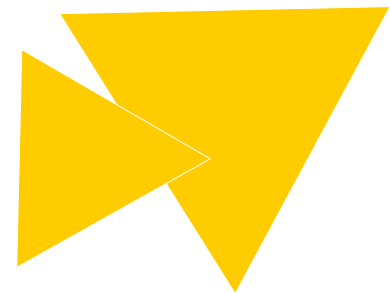


The Course at a Glance

- ▶ **Why should I learn how to encrypt?**
- ▶ **How to secure my browser**
- ▶ **Basics of smartphone security**

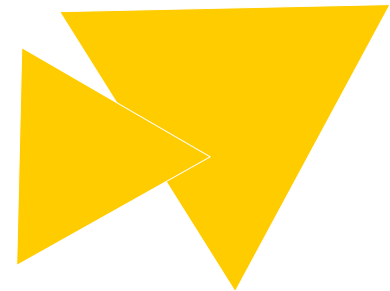


LET'S GO!

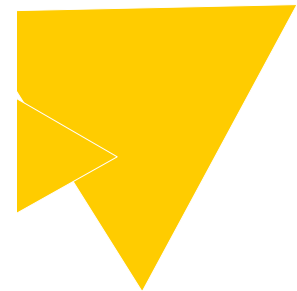


The Course at a Glance

- ▶ **Why should I learn how to encrypt?**
- ▶ **How to secure my browser**
- ▶ **Basics of smartphone security**

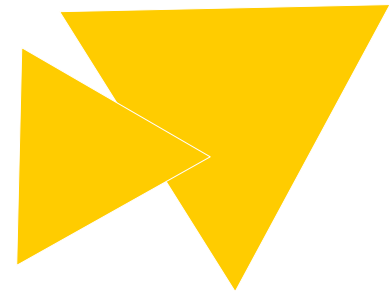


Digital Identity

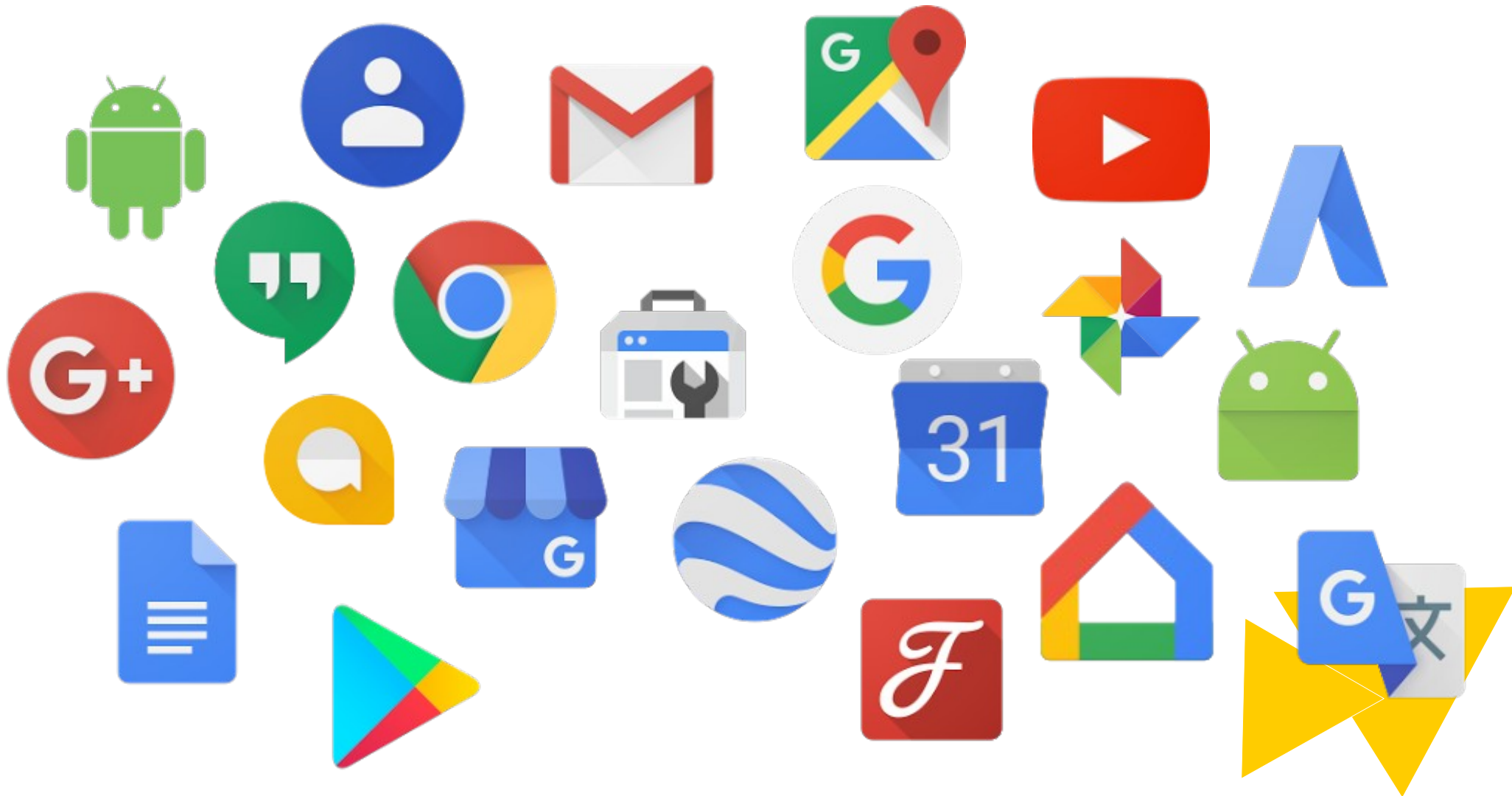


Metadata

- ▶ Search terms (Search History)
- ▶ Entered, seen, clicked
- ▶ IP address
- ▶ Language
- ▶ Date, time
- ▶ Device, operating system, browser
- ▶ Location (GPS or Browser)
- ▶ <https://myactivity.google.com/>



Google Services





**Zu niemandem ist man ehrlicher
als zum Suchfeld von Google.**

Constanze Kurz, Chaos Computer Club

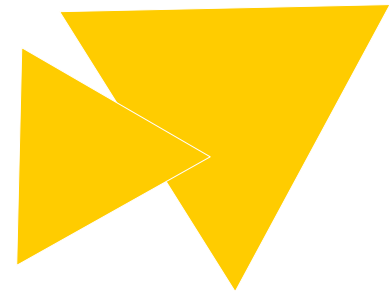
*To no one you are more honest
than to the search field of google.*

Privacy



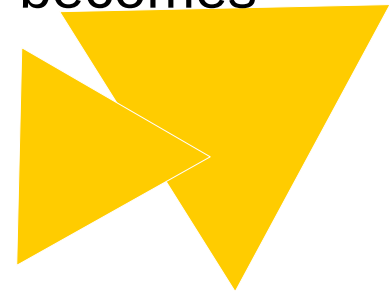
Why do we need privacy?

- ▶ „The right to be left alone.“
- ▶ Free development of personality
- ▶ Control over the consequences of one's own actions
- ▶ Self-determination (who knows what about me)
- ▶ Protection against criticism and discrimination
- ▶ Security (passwords, property,...)
- ▶ Freedom
- ▶ Intimacy?
 - ▷ **IMPORTANT FOR THE INDIVIDUAL**



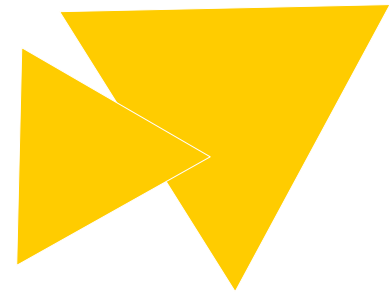
Why does a society need privacy?

- ▶ Important for our society
- ▶ Essential for democracy and the rule of law
 - ▷ Duty of confidentiality (medicine, law, advice, ...)
 - ▷ Journalism (protection of sources)
 - ▷ Right of defence against state power
- ▶ Social roles (different behaviour)
- ▶ Enabling progress (allowing opposition)
 - ▷ Once disclosure becomes the social norm, the opposite becomes the stigma
 - ▷ **IMPORTANT FOR SOCIETY**



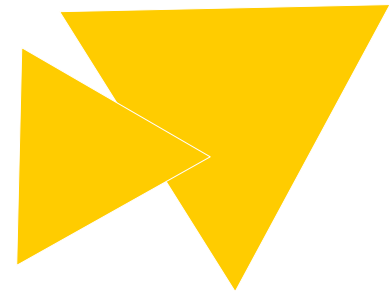
What if privacy is violated?

- ▶ Susceptibility to blackmail
- ▶ Chilling Effects



Privacy – what is it?

- ▶ "Something is private when you can control access to it."
(Rössler, 2001)



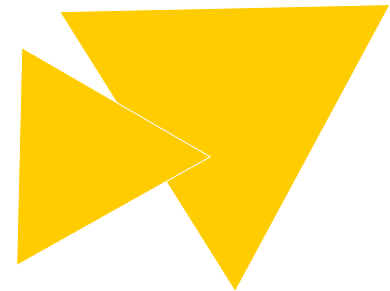
Privacy

▶ Analogue

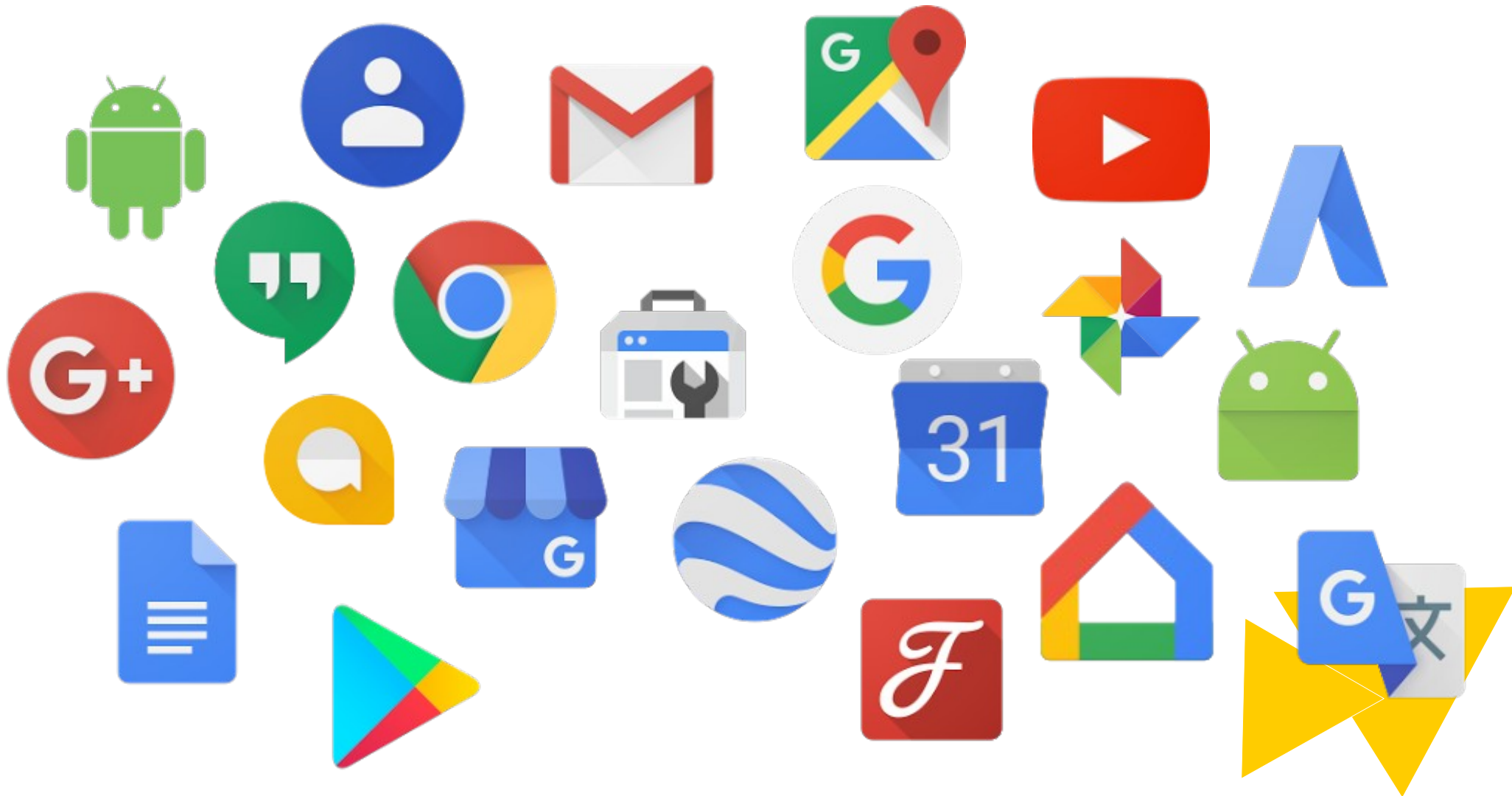
- ▷ Privacy naturally accepted
- ▷ Privacy violations mostly recognizable
- ▷ Privacy laws
 - Inviolability of the dwelling
 - Secrecy of correspondence
 - Free development of personality

▶ Digital

- ▷ New economic area
- ▷ New technical mechanisms/
possibilities
- ▷ Intransparent data collection
and use
- ▷ Technical understanding
often necessary
- ▷ Data protection laws not up
to date, #neuland

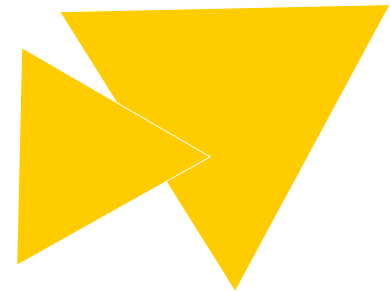


Google Services



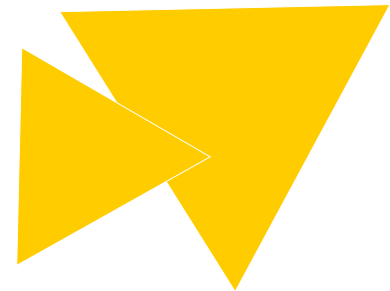
Google Analytics

- ▶ Integration on the website
- ▶ Statistics for the operators of the website
- ▶ Tracking of users when accessing the website
 - ▷ IP address, language, country
 - ▷ Date, time
 - ▷ Device, operating system, browser
 - ▷ Screen resolution
 - ▷ Referrer (from which website)



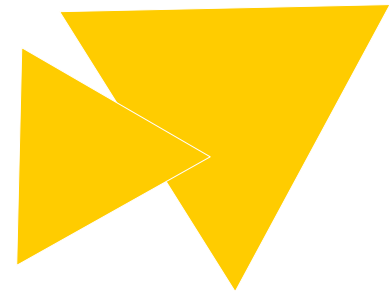
Which data does Facebook use?

- ▶ Place; Age; Gender; Educational level; Income and equity;
- ▶ House ownership and value; property size; house size in square meters;
- ▶ Users who are newly married; relationship status;
- ▶ Users planning to buy a car (what type/brand, and when);
- ▶ Operating system, email provider, type of internet connection;
- ▶ Users playing browser games;
- ▶ Users who have created a Facebook event;
- ▶ Number of credits;
- ▶ Users who actively use a credit card;
- ▶ Types of clothing purchased by the User's household;
- ▶ The time in the year in which the user's household buys the most;
- ▶ Users who buy "a lot" of beer, wine or spirits;
- ▶ Users who take medication for allergies and colds/flu,
- ▶ Pain killers and other non-prescription drugs
- ▶ Buying medicines;
- ▶ Users who are "receptive" to [advertising for] online
- ▶ Car insurance, university education or mortgages, prepaid
- ▶ Debit cards and satellite television;
- ▶ How long the user has lived in the house;
- ▶ Users likely to move soon;
- ▶ etc.



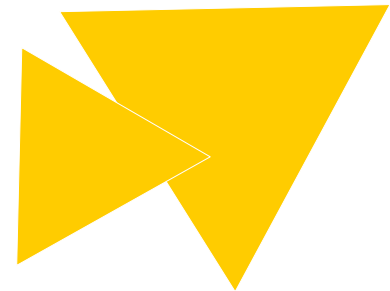
Facebook

- ▶ Free of charge
- ▶ Privacy settings are becoming more and more difficult
- ▶ Real name requirement
- ▶ Rights to the data
- ▶ Intransparency during transmission
- ▶ Lock-in (no profile export)



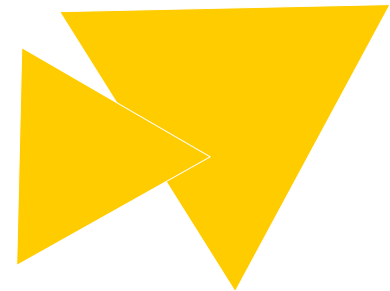
Data Economy

- ▶ "Free" offers
 - ▷ Data is a new currency
 - ▷ Data merchants buy profiles and sell them to the advertising industry, insurance companies, credit rating agencies, etc.
- ▶ Contained Systems
 - ▷ Proprietary Software
 - ▷ No open interfaces
- ▶ Big Data
 - ▷ Consolidation, analysis and evaluation of large amounts of data



Data Economy

- ▶ Security
 - ▷ means effort = expenses = money
- ▶ Data protection
 - ▷ Less data for the company
 - ▷ Less raw material to analyze and sell
 - ▷ Privacy "outdated"?
- ▶ The GDPR has made data protection strong again in Europe



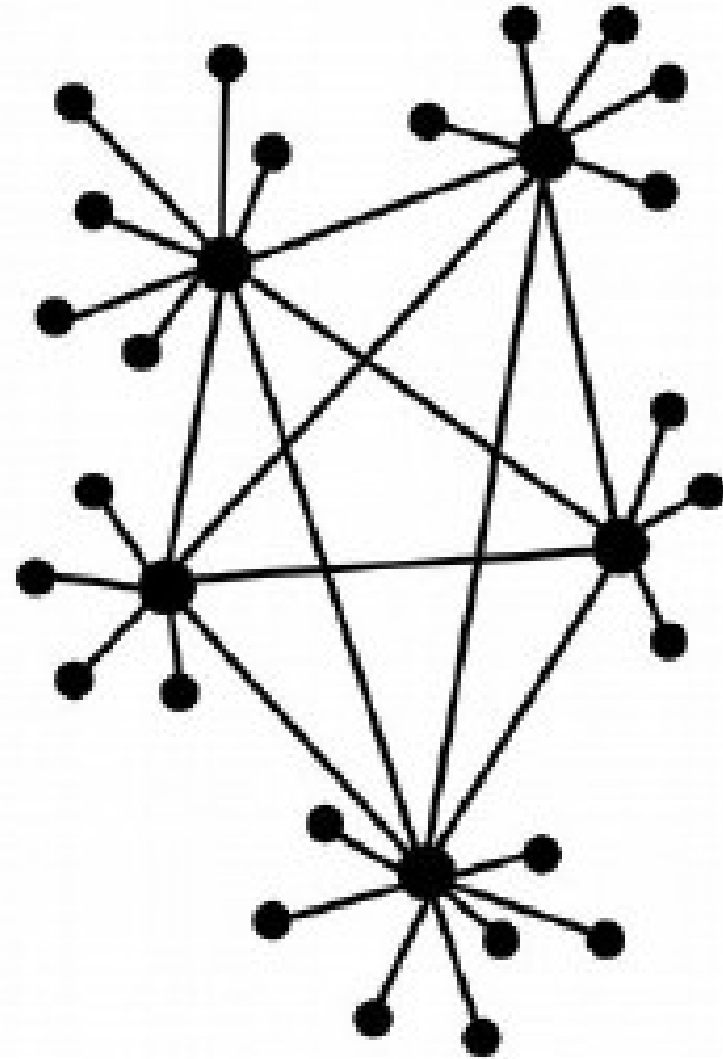
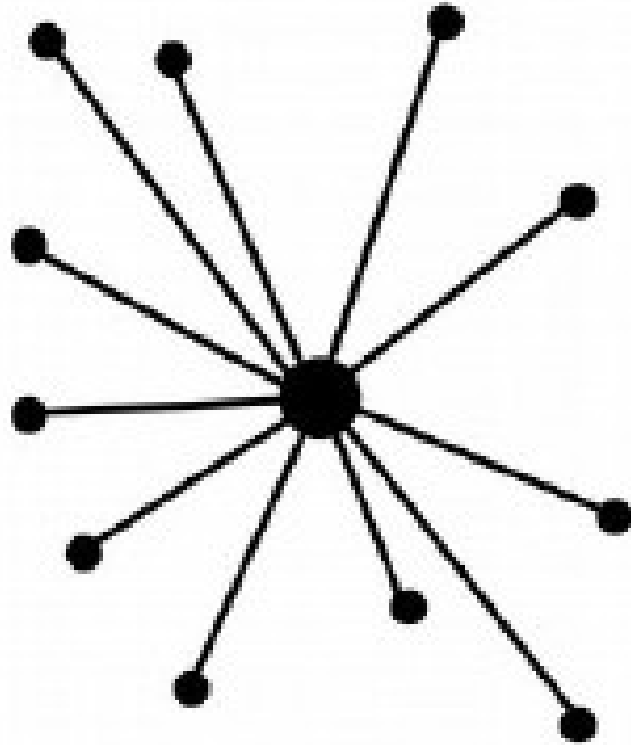
Facebook is watching you!

- ▶ Big Brother Award 2019 for *ZEIT ONLINE*, representative of about 3/4 of all online newspapers



Name	Startseite	Artikelseite	Aboseite
FAZ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Handelsblatt	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
taz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Neue Westfälische	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Westfalen-Blatt	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Centralized vs. decentralized



Metadata

- ▶ Content
- ▶ Metadata (message)
 - ▷ Sender, Recipient
 - ▷ Date, time
 - ▷ IP address / mobile network
- ▶ Metadata (photo)
 - ▷ disbandment
 - ▷ Aperture, exposure time
 - ▷ GPS coordinates

Lieber Max,

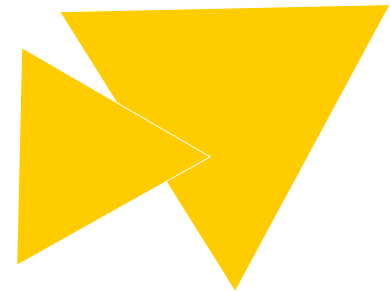
heute waren wir bei der Felsformation „Twelve Apostles“ im Süden von Australien. War mega beeindruckend!



Viele Grüße
Leah

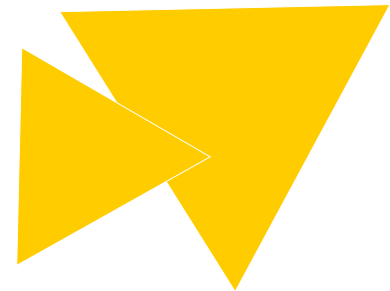
Metadata

- ▶ Often referred to as connection data in telecommunications.
- ▶ Small amount of data
- ▶ Easy to analyze (as opposed to content)
- ▶ Difficult to encrypt, as necessary to enable communication
- ▶ **Metadata is perfect for data analysis and mass monitoring!**



What are the problems of metadata?

- ▶ **Small amount of data, but a lot of knowledge about users:**
 - ▷ Interests, diseases, sexual preferences, movement profile, ...
- ▶ Easy to **analyze** (in comparison to content)
- ▶ **Consolidation** of data from different sources
 - ▷ Search, YouTube, Gmail, Analytics, AdWords, Android,...
- ▶ **Big Data:** Search trends (regional, worldwide)
- ▶ **Data trade:** advertising, creditworthiness, insurance...
- ▶ Difficult to encrypt because **necessary** to enable communication



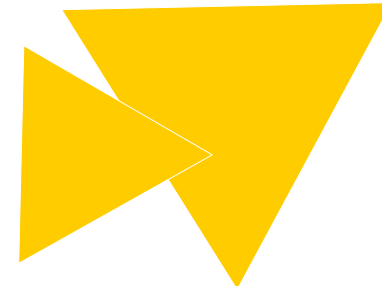
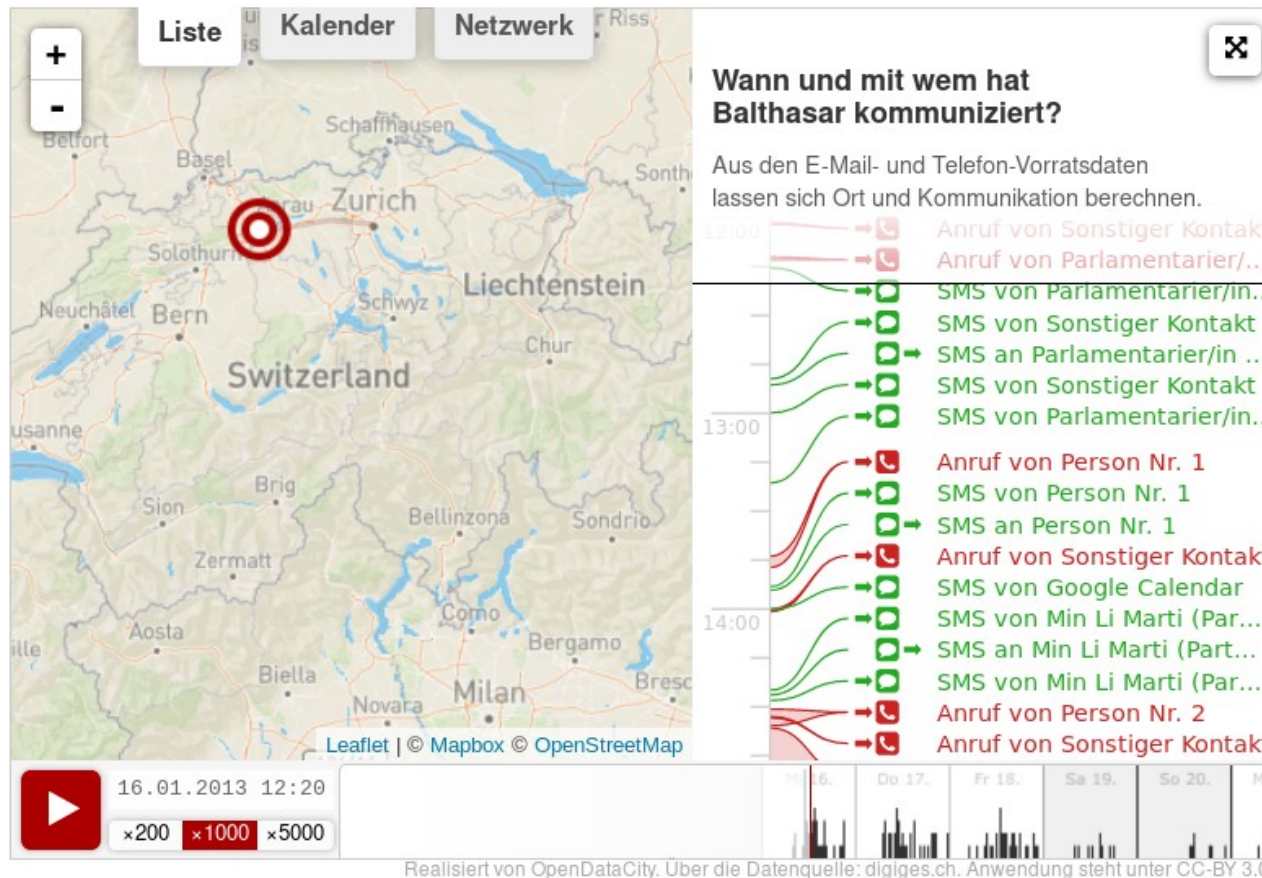


We Kill People Based on Metadata

General Michael Hayden, Ex-Chef von NSA und CIA

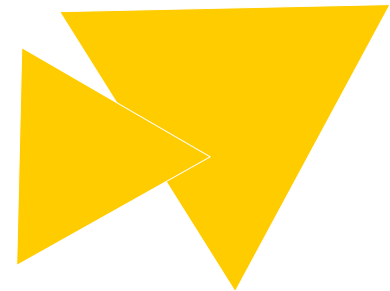
What does that mean?

- ▶ Balthasar Glättli (The Greens, Switzerland): <https://www.digitale-gesellschaft.ch/vorratsdatenspeicherung/>
- ▶ Malte Spitz (The Greens, Germany): <http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten>



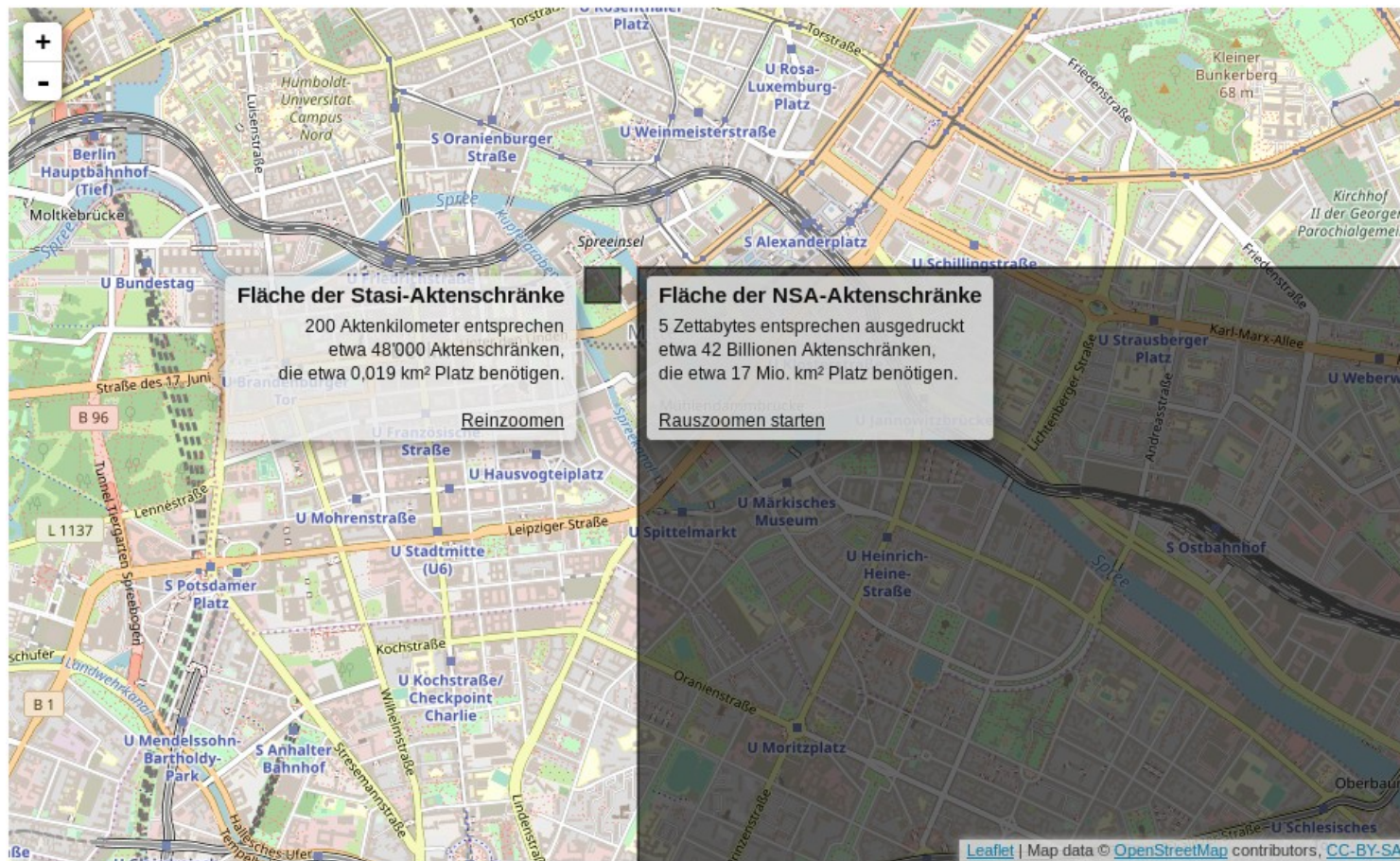
Consequences of surveillance

- ▶ All citizens are suspects
- ▶ Self-censorship
- ▶ Chilling effect → Appropriate behaviour
- ▶ Limitation of many fundamental rights:
 - ▷ Freedom of expression,
 - ▷ Privacy of correspondence,
 - ▷ Free development of personality



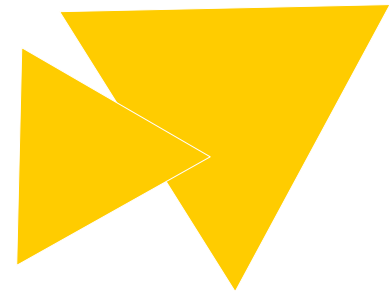
Mass surveillance by NSA

- ▶ Stasi vs. NSA area comparison: <https://apps.opendatacity.de/stasi-vs-nsa/>



The Course at a Glance

- ▶ **Why should I learn how to encrypt?**
- ▶ **How to secure my browser**
- ▶ **Basics of smartphone security**

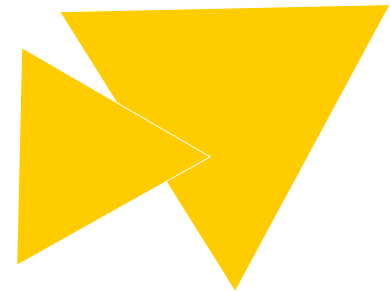
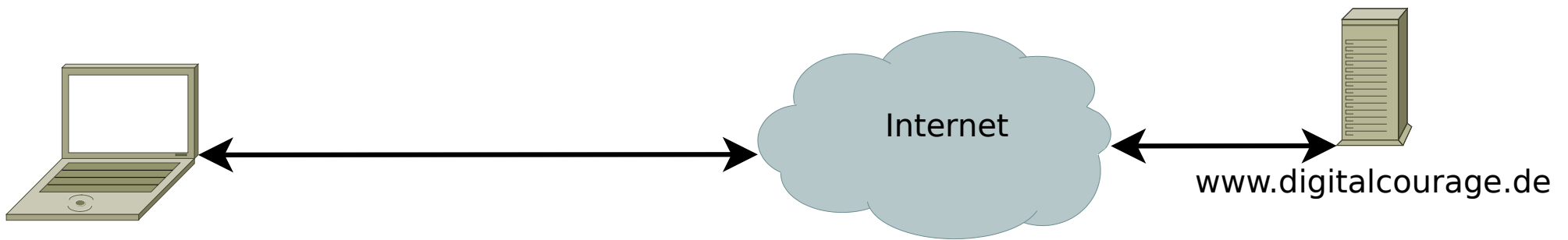


Browser Privacy

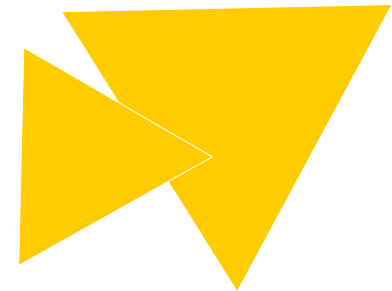
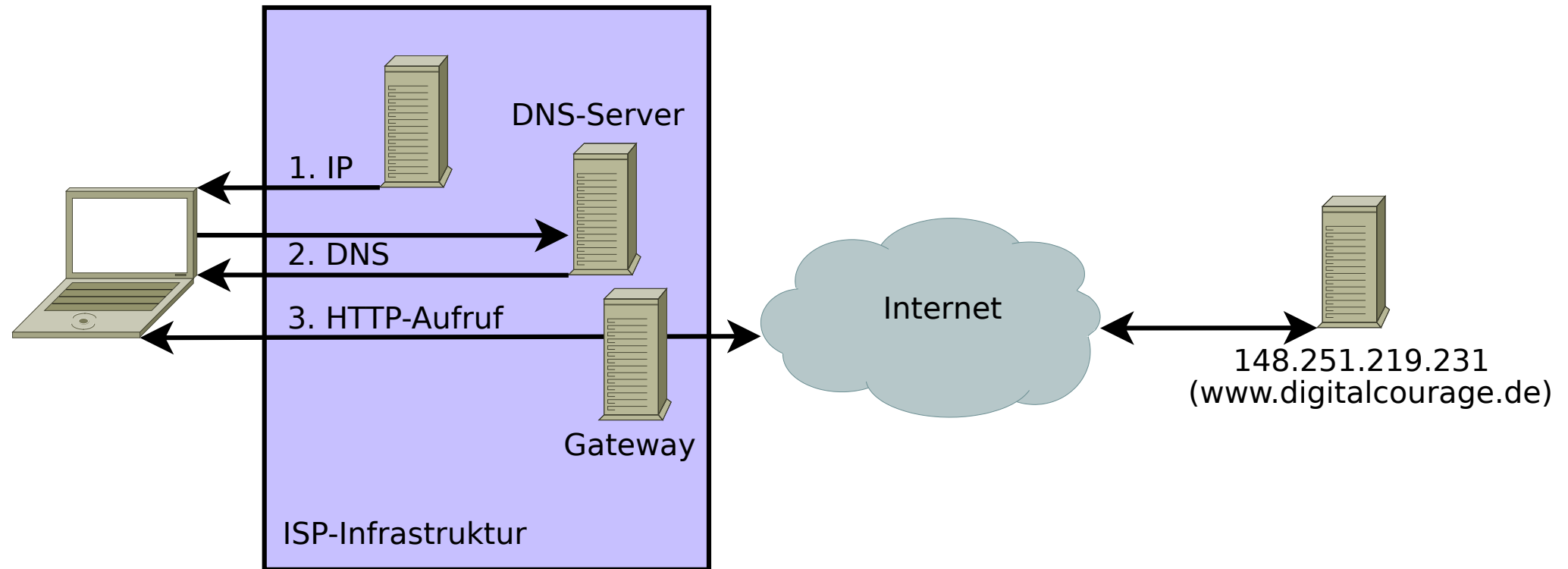
How does your browser support privacy?



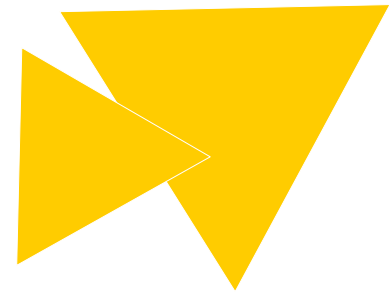
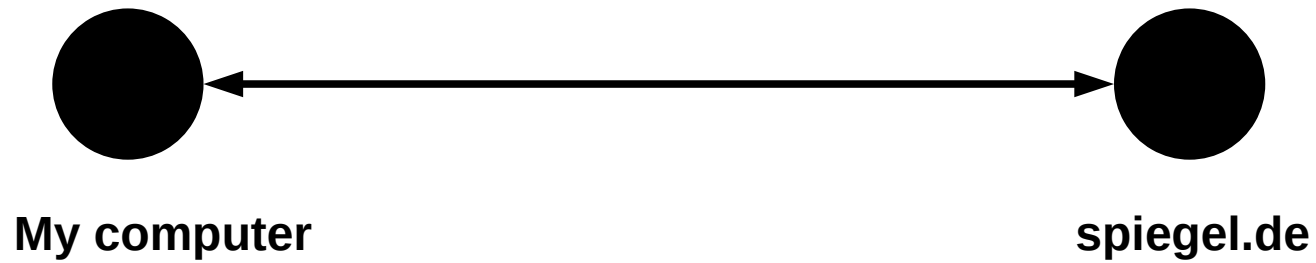
How does the internet work?



And technically?

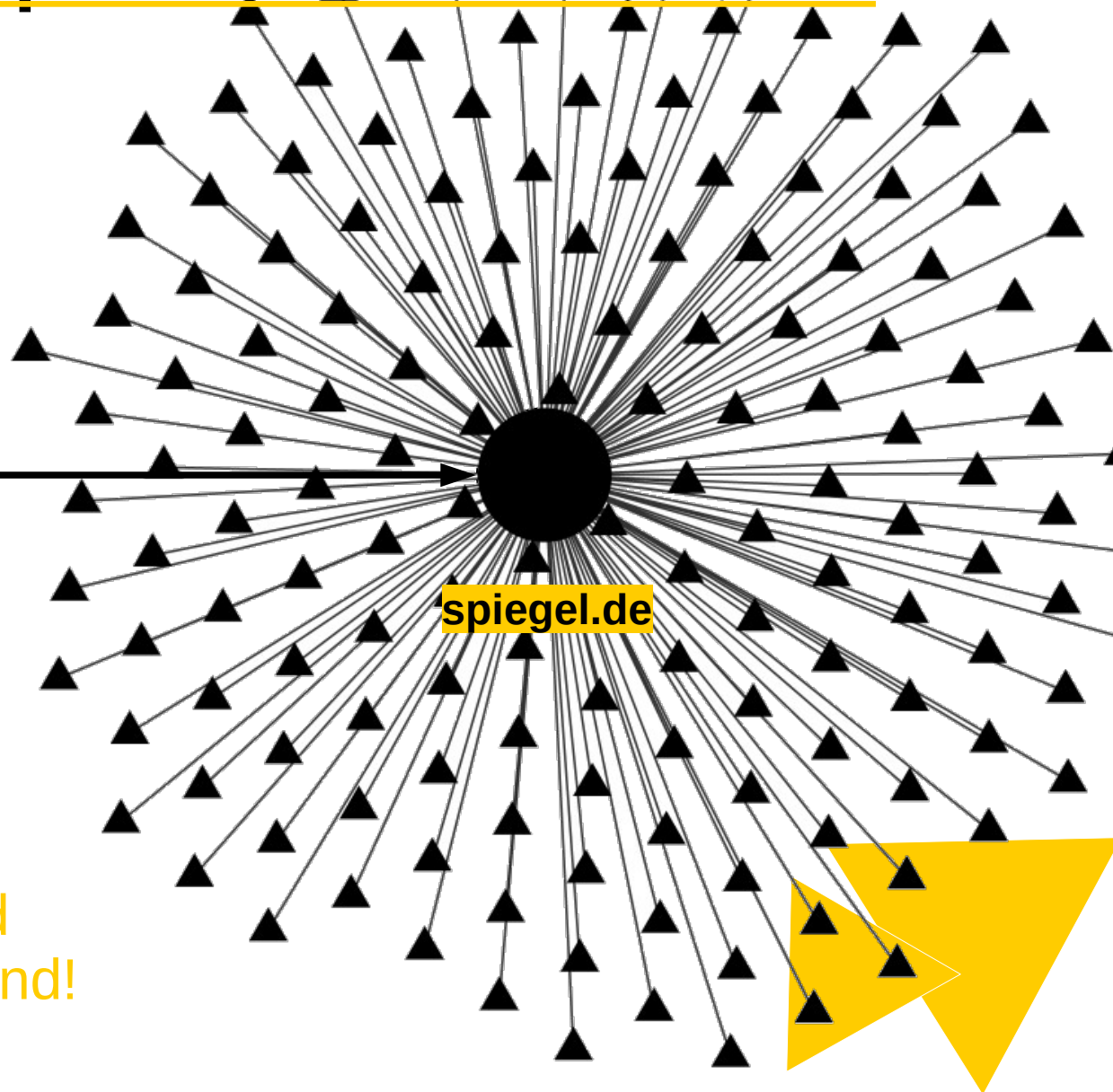


Let's visit [spiegel.de](https://www.spiegel.de)!

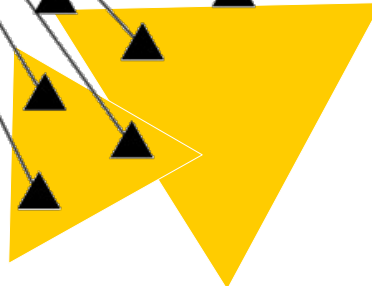


What does happen behind the scenes?

My
computer

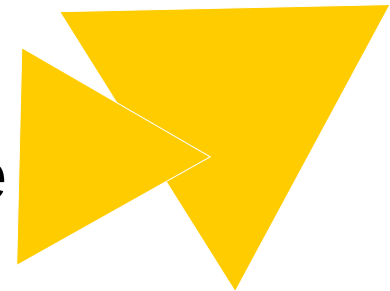


Sent requests to 152 third party websites the background!



How bad is it? Well...

- ▶ ioam.de, **google**tagmanager.com, omny.fm, cloudfront.net, mxcdn.net, optimizely.com, soundcloud.com, demdex.net, adalliance.io, emsservice.de, emetriq.de, criteo.net, s79.research.de.com, meetrics.net, omtrdc.net, criteo.com, **doubleclick**.net, hotjar.com, **google**-analytics.com, **google**tagservices.com, yieldlab.net, everesttech.net, xplosion.de, **google**apis.com, ampcid.**google**.com, adservice.**google**.de, ampcid.**google**.de, srv-2019-06-13-05.pixel.parsely.com, theadex.com, newrelic.com, adrtx.net, nr-data.net, ligatus.com, ligadx.com, summerhamster.com, zemanta.com, scorecardresearch.com, outbrain.com, **google**syndication.com, csi.**gstatic**.com, ... (ohne Subdomains!)



VISUALIZATION

Graph

DATA

Save Data

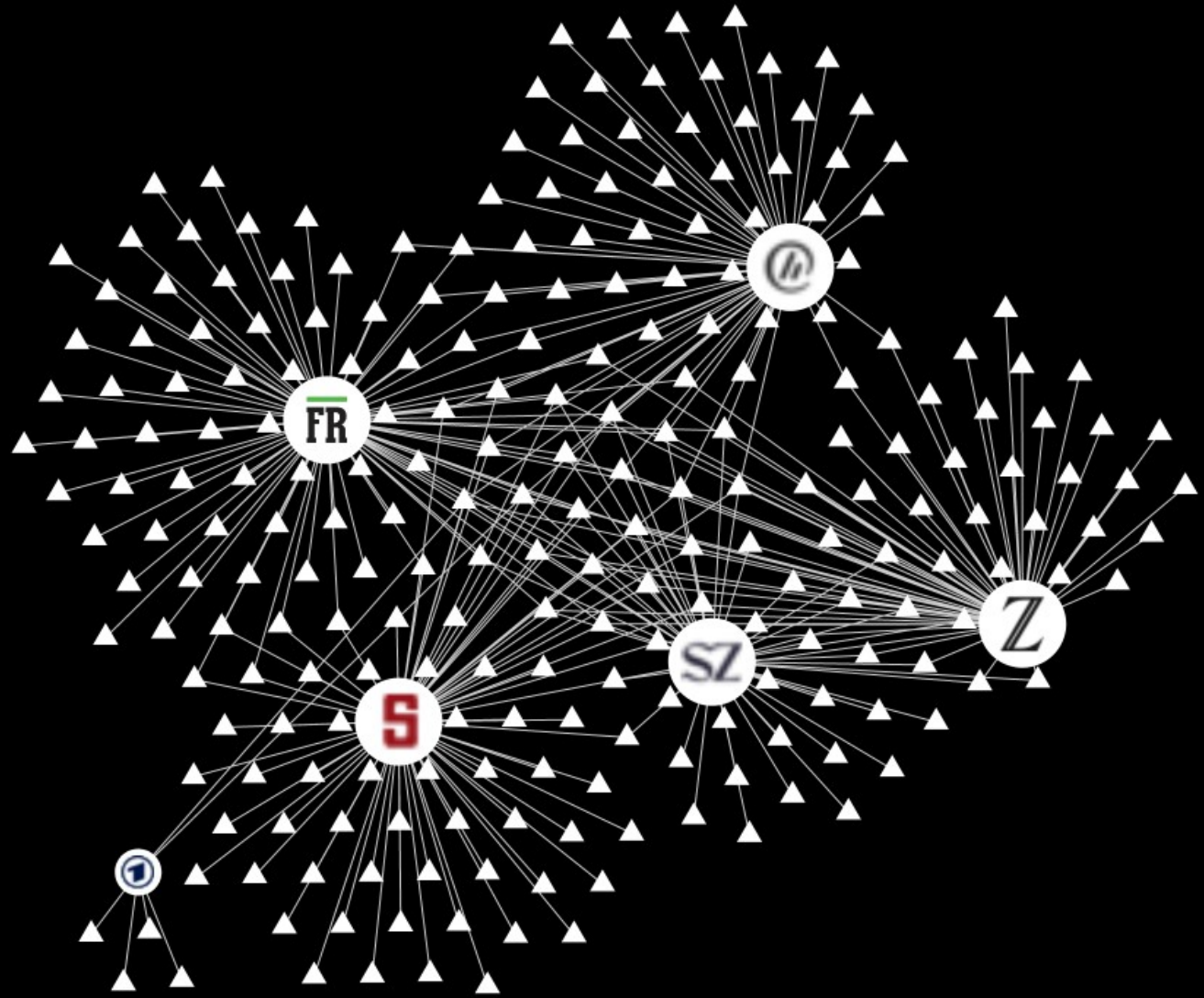
Reset Data

[Give Us Feedback](#)

Recent Site

GRAPH VIEW

netzpolitik.org



Comparison: with / without ad blocker

Todesfälle durch Listerien-Keime Wurst-Hersteller Wilke beantragt Insolvenz



Zwei Menschen sind gestorben, nachdem sie keimbelastete Wurst gegessen hatten. Nun ist das verantwortliche Fleischerei-Unternehmen Wilke insolvent. mehr...

Krise der Autobranche BMW kürzt Spitzenkräften die Bezüge



BMW steckt in der Krise und spart beim Personal. Hochqualifizierten Mitarbeitern werden die Gehälter um bis zu 14.000 Euro gekürzt. Der Betriebsrat kündigt Gegenwehr an - die Arbeit werde ja nicht weniger. mehr... [Forum]

Auto der Zukunft: Habeck kritisiert VWs Elektro-Strategie

Ostdeutschland 30 Jahre nach dem Mauerfall Ist doch alles echt super gelaufen



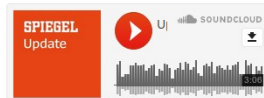
Von wegen "blühende Landschaften" - die Deutsche Einheit ist zum Desaster geworden. Aussprechen will das in der Politik vor lauter Staatsräson aber kaum jemand. Die Quittung kommt jetzt, bei den Wahlen. Eine Kolumne von Thomas Fricke mehr... [Forum]

SCHLAGZEILEN >

Alle Artikel auf einen Blick...

SPIEGEL Hier finden Sie alle Artikel

SPIEGEL Update: Nachrichten zum Hören >



Abonnieren

Mehr Infos

Top Gelesen | Versickt | Gesehen

1 Reaktionen auf Trumps Bitte an

DIE PLATINUM CARD AUS METALL.


verlängert bis 13.10.

300 Euro Aufnahmegebühr sparen

200 Euro jährliches Online-Reiseguthaben

200 Euro jährliches SIXT ride Fahrtguthaben



SPIEGEL ONLINE SPIEGEL 

Anmelden

Menü | Politik | Meinung | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | mehr ▾

4. Oktober 2019 Schlagzeilen | DAX 11.972,18 | Abo



Todesfälle durch Listerien-Keime Wurst-Hersteller Wilke beantragt Insolvenz



Zwei Menschen sind gestorben, nachdem sie keimbelastete Wurst gegessen hatten. Nun ist das verantwortliche Fleischerei-Unternehmen Wilke insolvent. mehr...

Krise der Autobranche BMW kürzt Spitzenkräften die Bezüge



BMW steckt in der Krise und spart beim Personal. Hochqualifizierten Mitarbeitern werden die Gehälter um bis zu 14.000 Euro gekürzt. Der Betriebsrat kündigt Gegenwehr an - die Arbeit werde ja nicht weniger. mehr... [Forum]

Anzeige



AM EX
BESTE Fremde Kreditkarte

CHIP
sehr gut

Handkitten
BESTE Kreditkarten

 digitalcourage
Hochschulgruppe

Comparison: with / without ad blocker

▶ Just what I want to see now

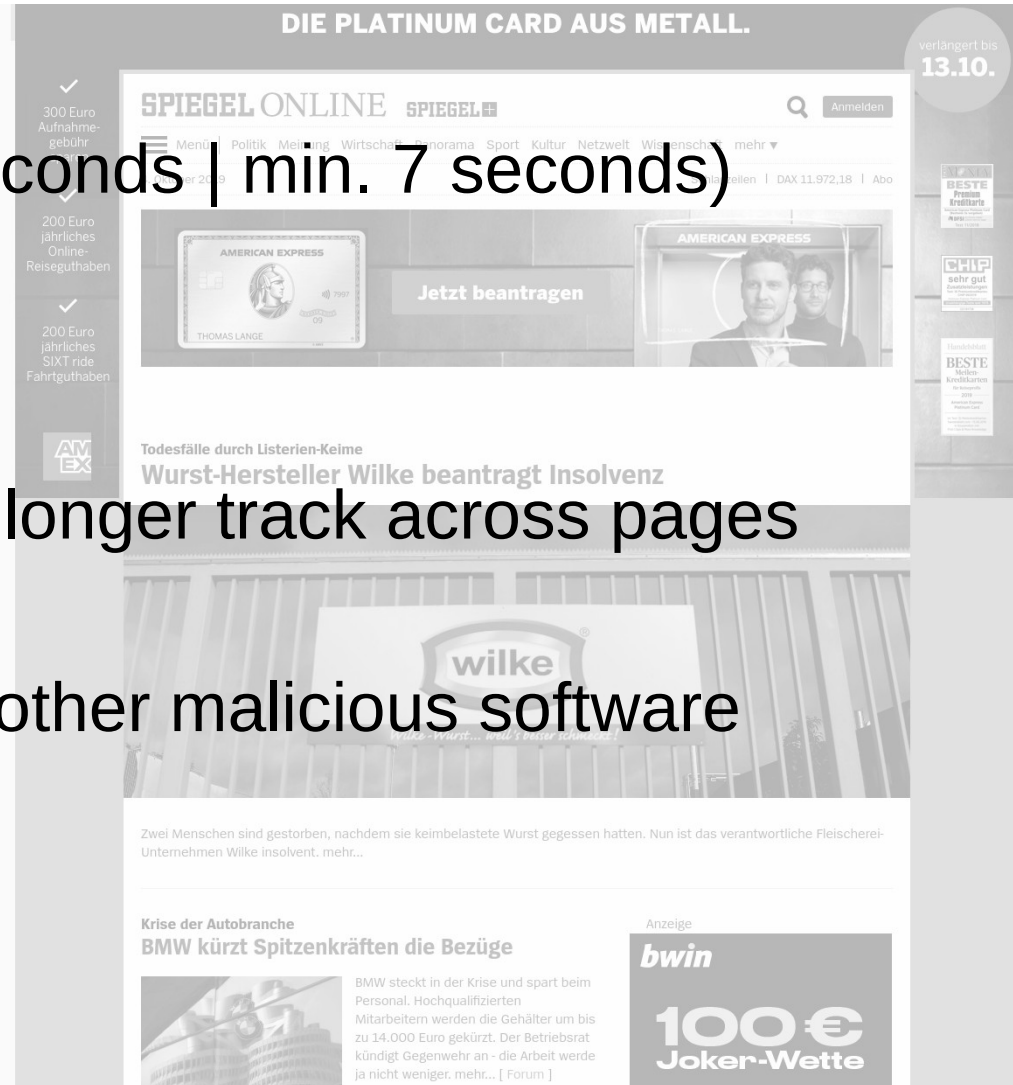
▶ Page loads faster (max. 2 seconds | min. 7 seconds)

▶ Saves data volume

▶ environmental protection

▶ Advertising networks can no longer track across pages (tracking)

▶ Reduced risk of viruses and other malicious software




verlängert bis 13.10.

BESTE Finanz-Trendkarte
CHIP sehr gut
BESTE Kreditkarten-Anbieter


VISUALIZATION

 Graph

DATA

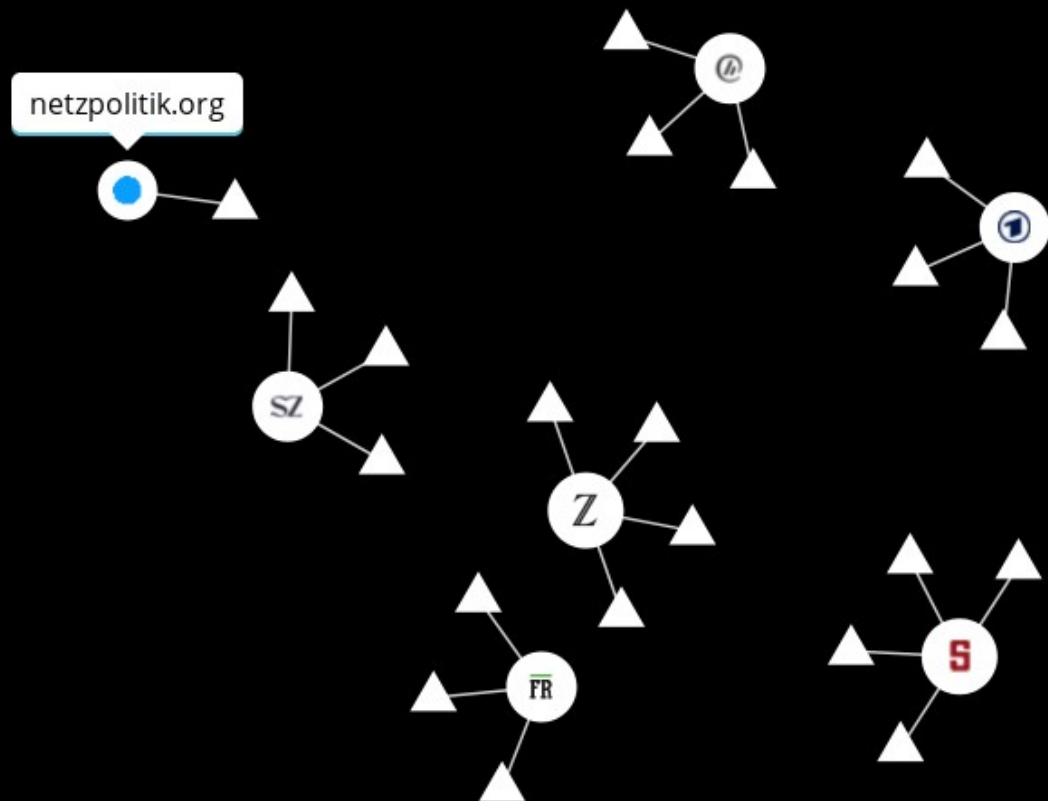
 Save Data

 Reset Data

 [Give Us Feedback](#)

Recent Site

GRAPH VIEW





🌐 Webbkoll is also available in [German](#) (auf Deutsch), [Norwegian](#) (norsk) and [Swedish](#) (svenska)!

Check your site!

This tool helps you check what data-protecting measures a site has taken to help you exercise control over your privacy.

Please note:

1. This tool simulates a normal browser visit with Do Not Track disabled (browser default) and with no add-ons.
2. Even if you enter https://, http:// will be checked, to see if it redirects to https:// automatically (redirects are followed).
3. Generally things work, but some sites (sometimes) don't work for various reasons.
4. The backend is currently running on a single server with limited resources, so in case of usage spikes, waiting times can be long. (But you can [run your own instance!](#))
5. Feedback is appreciated: send [email](#) or [open an issue](#).

<https://webbkoll.dataskydd.net/>



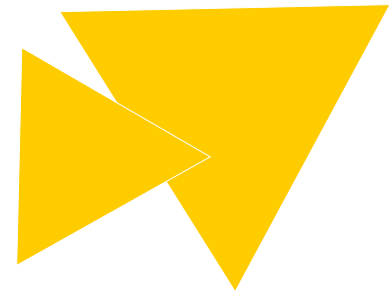
"Here's how we take back the
Internet."

– Title of a TED Talk by Edward Snowden

Safe surfing with privacy

What do we want?

- ▶ Security:
 - ▷ privacy
 - ▷ authenticity
 - ▷ integrity
- ▶ Anonymity
 - ▷ Only partially compatible with authenticity!
- ▶ Resistance to censorship



How do we get there?

What do we want?

- ▶ Security:
 - ▷ privacy
 - ▷ authenticity
 - ▷ Integrity
- ▶ Anonymity
- ▶ Only partially compatible with authenticity!
- ▶ Resistance to censorship

Let's go!

- ▷ HTTPS (encryption)
- ▷ HTTPS (certificates)
- ▷ HTTPS

- ▷ Firefox
- ▷ Block tracking
- ▷ Only necessary cookies
- ▷ Tor Browser



How can a web server identify and track me?

▶ Cookies

- ▷ Small text files that the website can save in the browser and retrieve again.

▶ Browser and operating system features:

- ▷ Browser type and version, operating system, language
- ▷ Fonts, browser add-ons (NoScript, Flash, ...),
- ▷ Browser window size, font rendering, and much more.

▶ External features:

- ▷ IP address

▶ Unique browser fingerprint: ***<https://panopticklick.eff.org>***





PANOPTICCLICK

Is your browser safe against tracking?

How well are you protected against non-consensual Web tracking? After analyzing your browser and add-ons, the answer is ...

Yes! You have **strong protection against Web tracking** though your software isn't checking for Do Not Track policies.

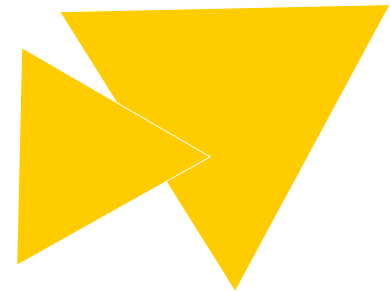


Your browser fingerprint appears to be unique among the 6,341,198 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 22.6 bits of identifying information.**

How can I protect myself from tracking?

- ▶ Browser choice: Firefox
- ▶ Browser settings
 - ▷ Block page elements, activity tracking, third-party cookies, identifiers
 - ▷ Always send "Do Not Track" information
- ▶ Search engines
 - ▷ Startpage.com, Qwant.com, MetaGer.de (in contrast to Google no individualized results)
- ▶ Disable JavaScript if possible
- ▶ Use browser add-ons (but wisely!)
- ▶ Learn how to check your network traffic



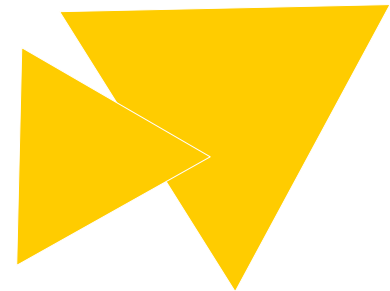
Use FREE SOFTWARE

- ▶ **Freedom 0:** The freedom to execute the program as you wish, for any purpose.
- ▶ **Freedom 1:** The freedom to study the functioning of the program and to adapt it to one's own data processing needs.
- ▶ **Freedom 2:** The freedom to redistribute the program and thus help others.
- ▶ **Freedom 3:** The freedom to improve the program and to release these improvements to the public so that the whole community benefits.
- ▶ ⇒ Much more than just Open Source (reveal source code)

Firefox add-ons

For beginners

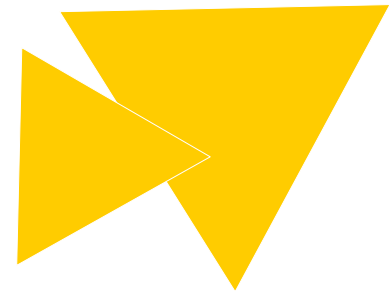
- ▶ Block ads and trackers: **uBlock origin**
- ▶ Replace JavaScript libraries: **Decentraleyes**
- ▶ Always encrypt website traffic: **HTTPS Everywhere**
- ▶ Automatically delete Cookies: **Cookie AutoDelete**
- ▶ Delete or deactivate Adobe Flash
- ▶ Block active content **NoScript**
 - ▷ Allow everything except JavaScript (for beginners)



Firefox add-ons

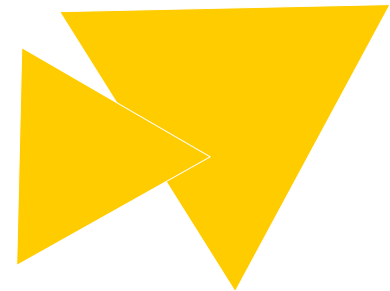
For advanced users

- ▶ Block referers: **SmartReferer**
- ▶ Block everything (clear whitelist): **NoScript**
- ▶ Block all third party requests: **uMatrix**



Monitor the effects

- ▶ Check the effects of add-ons and settings:
 - ▷ Menu → Web Developer → Network



Important: Private Mode

- ▶ No storage of data of visited websites on your own computer (no history, no URL completion, cookies, etc.)
- ▶ No traces remain on the local system
- ▶ BUT: No anonymity in the internet

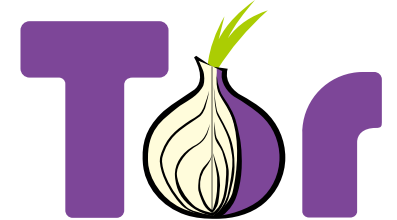


You're in a Private Window

Firefox clears your search and browsing history when you quit the app or close all Private Browsing tabs and windows. While this doesn't make you anonymous to websites or your internet service provider, it makes it easier to keep what you do online private from anyone else who uses this computer.

[Common myths about private browsing](#)

Browse anonymously with Tor



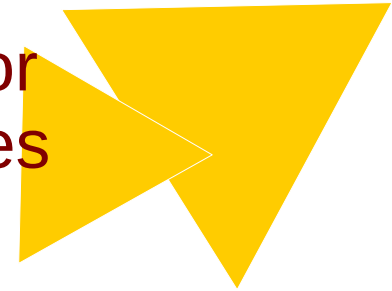
- ▶ Normal browsing
 - ▷ Both sides see their counterparts directly
- ▶ Browsing with Tor
 - ▷ All data traffic passes through the Tor network
 - ▷ Only the gateway node of the Tor network "knows" me
 - ▷ The website you are surfing on has no possibility to find out your origin (IP address)

Advantages

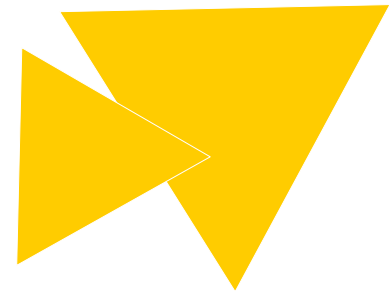
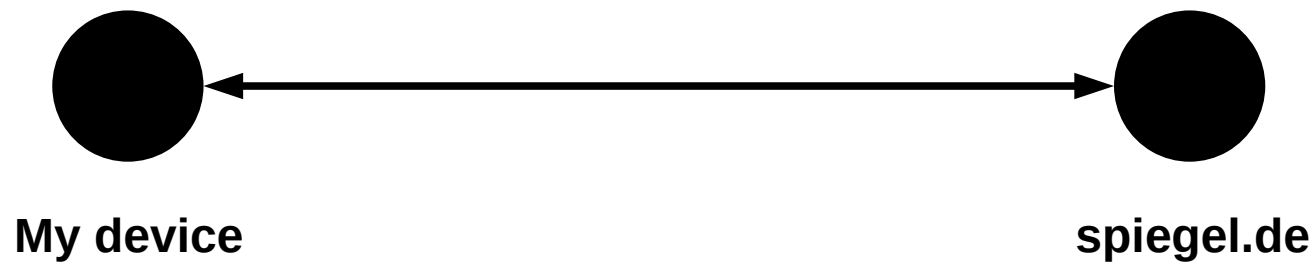
- ▶ Open Source, Free Software
- ▶ Anonymous Surfing

Disadvantages

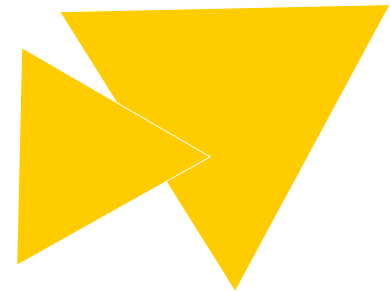
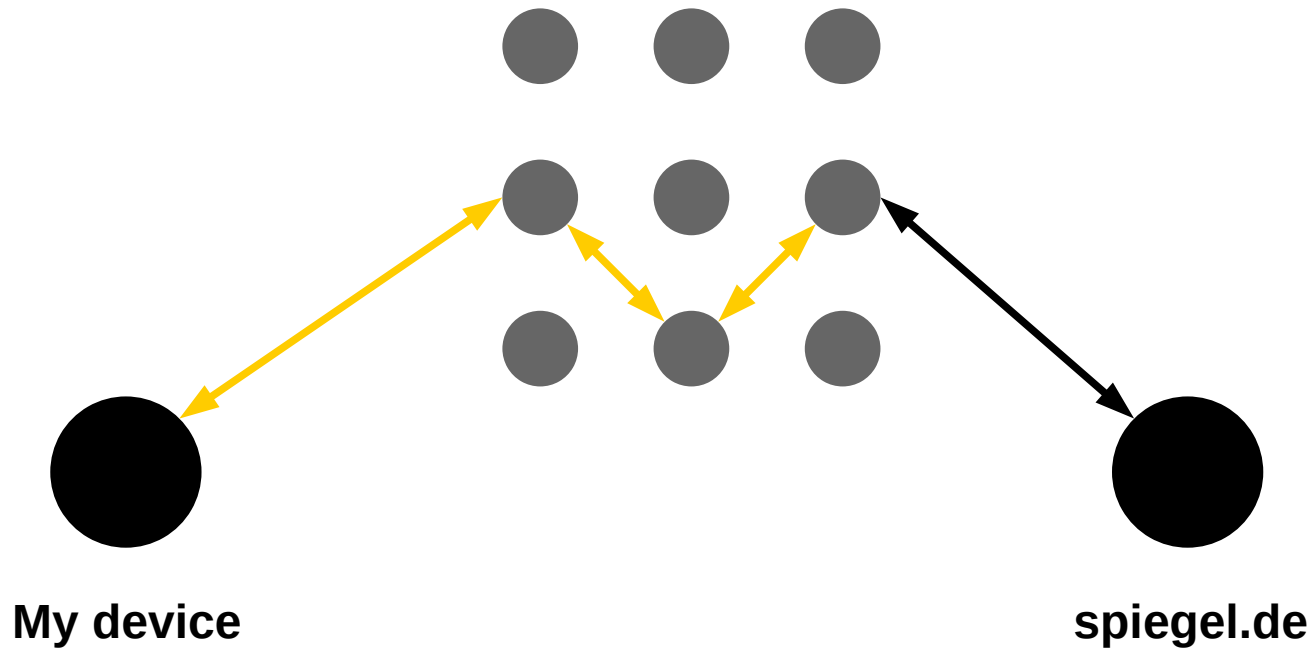
- ▶ Login not useful for personalized pages
- ▶ Slower



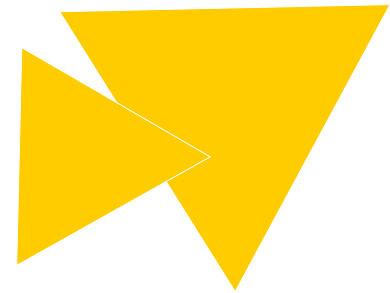
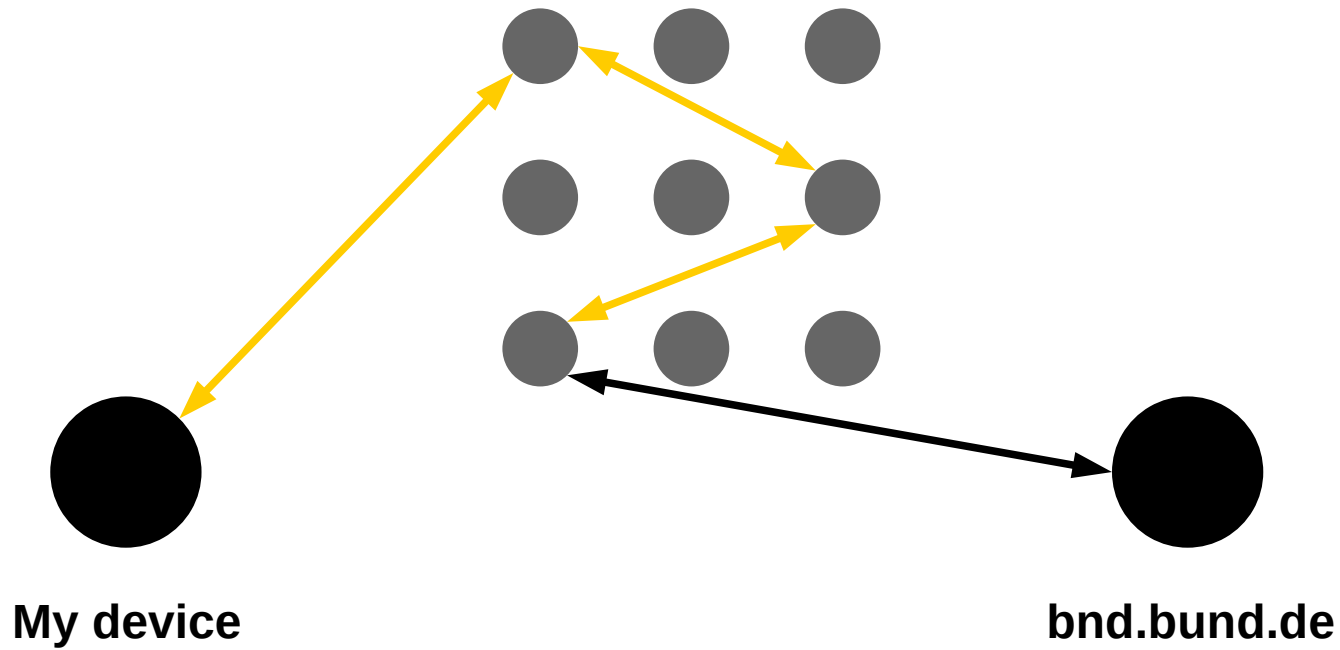
How does the Internet work?



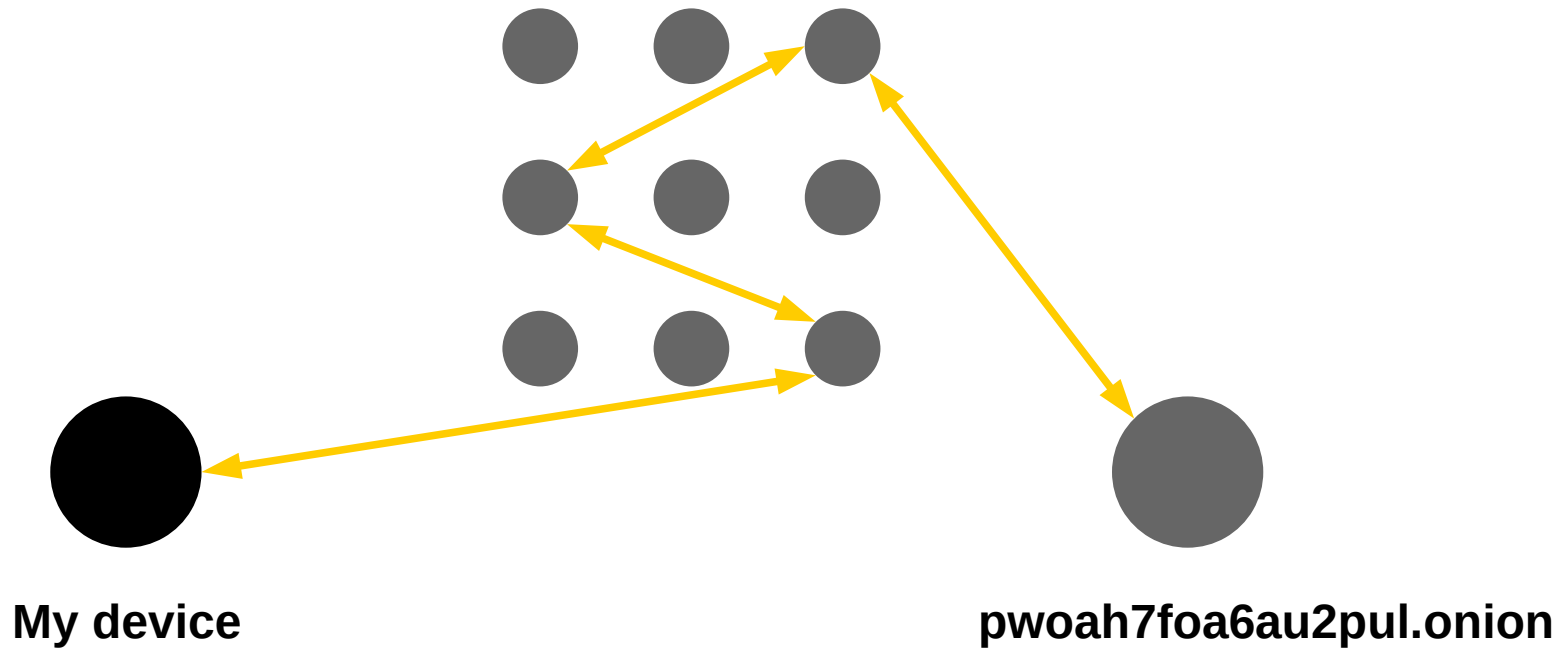
How does Tor work?



How does Tor work?

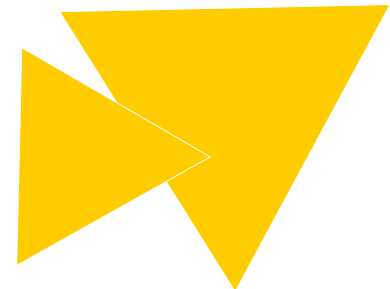


Excursus: Darknet



▶ Possible Darknet pages / services:

- ▷ Marketplaces
- ▷ email provider
- ▷ file sharing
- ▷ forums
- ▷ ...



How to use Tor?

▶ Install Tor Browser

- ▷ Modified Firefox from multiple addons
- ▷ (NoScript, HTTPS Everywhere, Torbutton and TorLauncher)
- ▷ <https://www.torproject.org/download/>

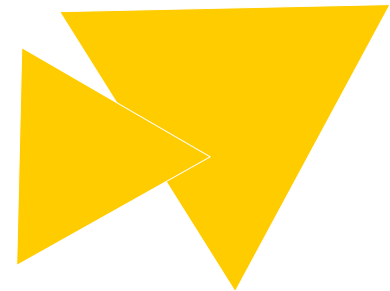
▶ Note about the target group:

- ▷ Use is particularly useful for exposed persons (investigative journalists, within certain countries with censored Internet or other oppression, ...).
- ▷ For the normal user, the use of advertising blockers and possibly further addons is often sufficient.



Download Tor Browser

- ▶ Firefox + Tor + NoScript + HTTPS-Everywhere
- ▶ Download via: <https://www.torproject.org/>



About Tor - Tor Browser

About Tor

Tor Browser Search with Disconnect or enter address

Search

Security Level : Standard

Tor Browser 8.5.1
[View Changelog](#)

Explore. Privately.

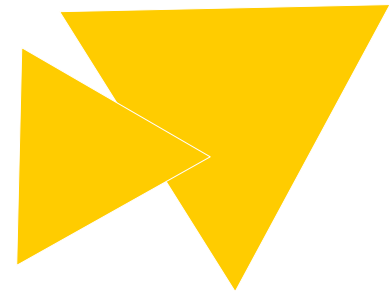
You're ready for the world's most private browsing experience.

Search with DuckDuckGo

Keep Tor strong. [Donate Now](#) »

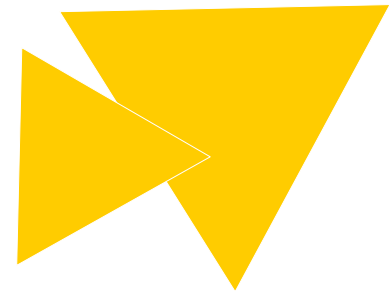
Tails – an operating system for Tor

- ▶ The **A**mnestic **I**ncognito **L**ive **S**ystem (Tails)
- ▶ Live-Linux-DVD / USB
- ▶ Anonymity as first design principle
- ▶ Many Tools
 - ▷ Pidgin
 - ▷ electron
 - ▷ MAT
 - ▷ KeePassXC



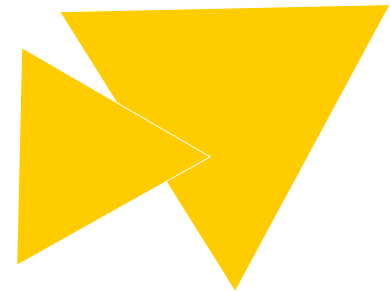
Thank you for listening.

Let's try that!



The Course at a Glance

- ▶ **Why should I learn how to encrypt?**
- ▶ **How to secure my browser**
- ▶ **Basics of smartphone security**



And yet again: Metadata

▶ What is metadata?

- ▷ „Data about data“
- ▷ Example SMS: length of the message, time, location (cell tower), sender, receiver
- ▷ Metadata often provide more valuable information about people than the actual content

→ Especially interesting for secret services:

- In 2015 the German BND stored 220 Millionen metadata units – **daily**.

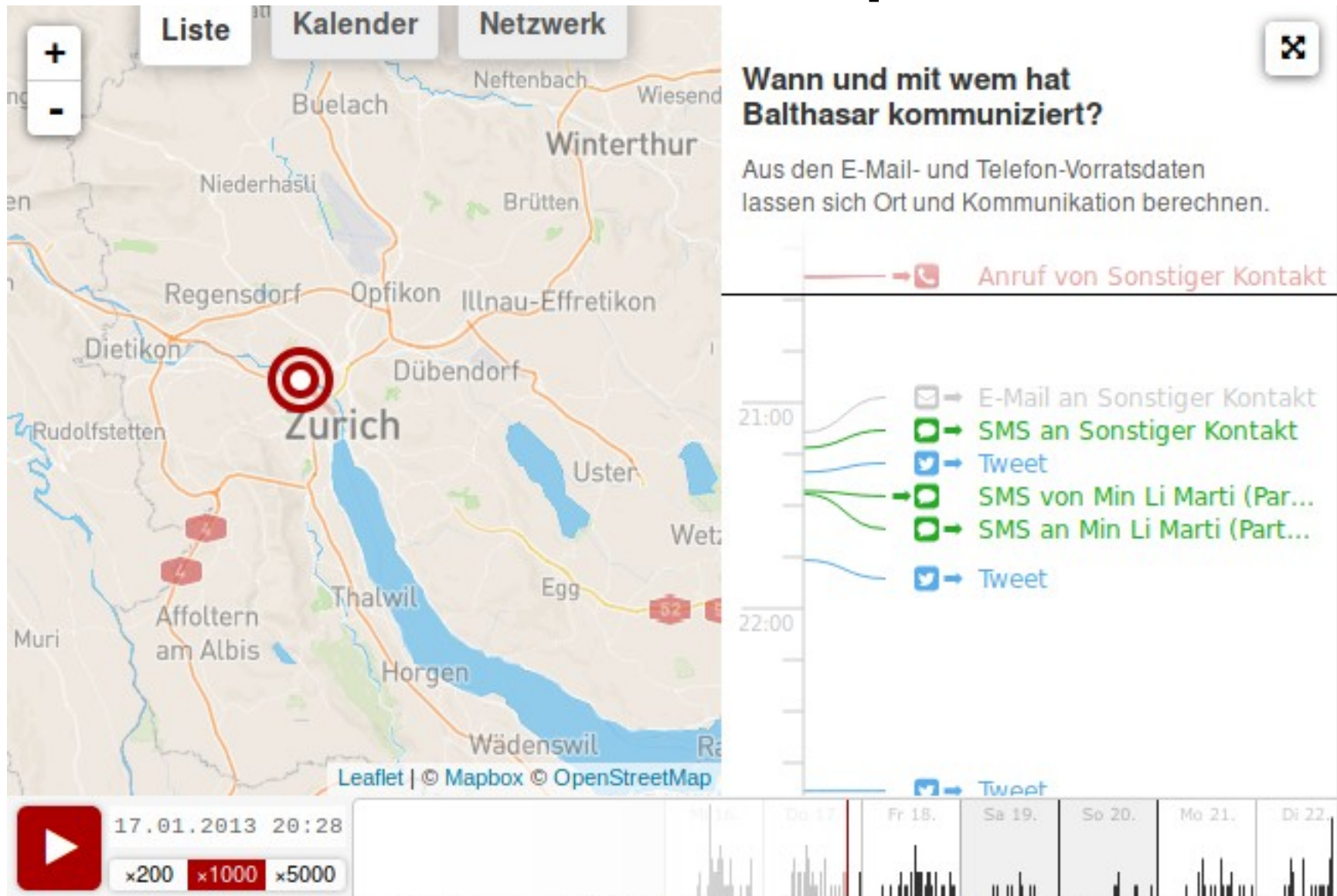


Surveillance

- ▶ Secret services analyze meta data by certain criteria ...
(contact relationships, travel data, financial transactions, ...)
- ▶ ... and use them against people:
(e.g. in the Ukraine in early 2014. SMS to participants of an demonstration:
„Dear subscriber, you are registered as a participant in a mass disturbance.“)



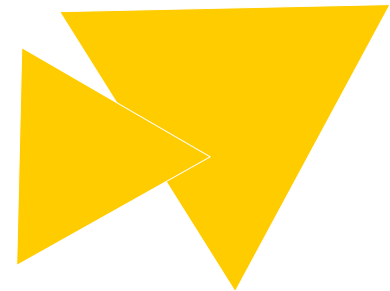
Treacherous smartphone



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

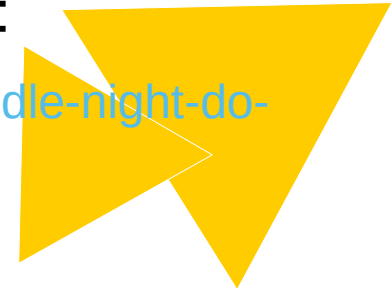
Commercial data collections

- ▶ Market for optimized personalized advertisements
- ▶ Apps collect diverse user data (e.g. location data) and forward them to third parties
- ▶ Example: In a test by privacy blogger Mike Kuketz the diabetic app **mySugr** sent data to the US-based analytics company Mixpanel.
 - ▷ Email address
 - ▷ Full name of the user
 - ▷ Diabetes type
 - ▷ Therapy type (syringe oder pump)



Smartphones: hardware & operating system

- ▶ Hardware („super wiretap“)
 - ▷ Microphone, camera, GPS, light sensor, acceleration sensor, NFC Wi-Fi, Bluetooth and more
- ▶ Operating system iOS: The golden cage by Apple
 - ▷ Apps from a central source (App Store)
 - ▷ Closed system, user not in control ("Gerätehoheit")
 - ▷ More freedom by „jailbreaking“ → root access
 - ▷ Massive amount of tracking by apps from the App store:
 - <https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/>



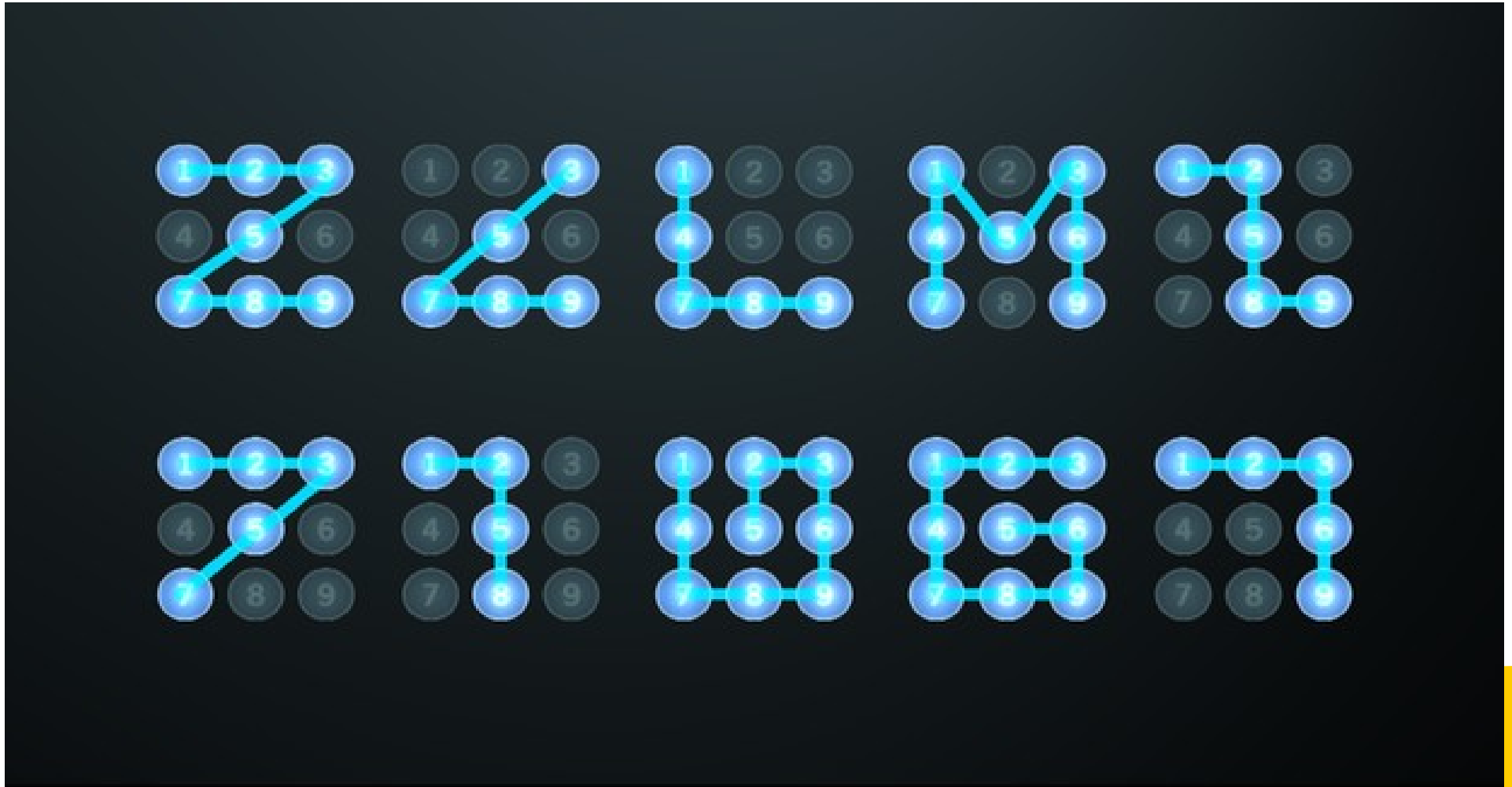
Android

- ▶ Good foundation in theory ...
 - ▷ Linux-based, Free Software

- ▶ **But:**
 - ▷ New devices come with preinstalled and tightly integrated Google services: Search, Chrome, Gmail, Maps, data synchronization ...
 - ▷ Play Store
 - ▷ Remote access, data collection and transmission
 - ▷ No root access by default
 - ▷ Often terrible manufacturer support regarding system and security updates, development dependent on Google

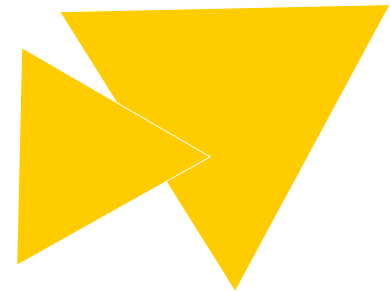


Typical lock patterns



First steps: configuration

- ▶ Setting up a secure screen lock:
 - ▷ From unsecure to secure:
swipe, pattern, fingerprint/iris, PIN, password
- ▶ Disable Wi-Fi, GPS, Bluetooth etc., when not in use
- ▶ Install and configure Mozilla Firefox



Secure device unlocking by iris scanning?



App permissions: Facebook (1)

▶ Identity

- ▷ read your own contact card
- ▷ find accounts on the device
- ▷ add or remove accounts

▶ Photos/Media/Files

- ▷ modify or delete the contents of your USB storage
- ▷ read the contents of your USB storage

▶ Camera

- ▷ take pictures and videos
- ▷ Device ID & call information
- ▷ read phone status and identity

▶ Calendar

- ▷ read calendar events plus confidential information
- ▷ add or modify calendar events and send email to guests without owners' knowledge

App permissions: Facebook (2)

▶ Storage

- ▷ modify or delete the contents of your USB storage
- ▷ read the contents of your USB storage

▶ Device & app history

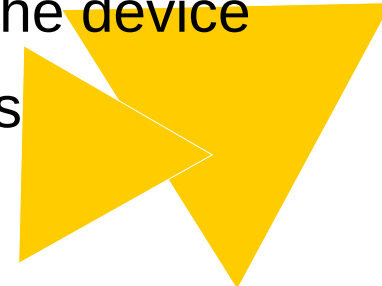
- ▷ retrieve running apps

▶ Phone

- ▷ write call log
- ▷ directly call phone numbers
- ▷ read phone status and identity
- ▷ read call log

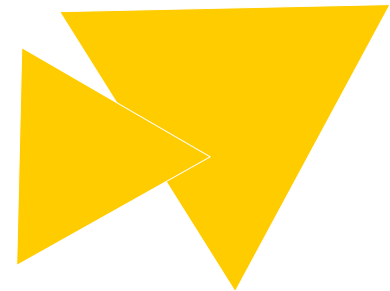
▶ Contacts

- ▷ modify your contacts
- ▷ find accounts on the device
- ▷ read your contacts



App permissions: Facebook (3)

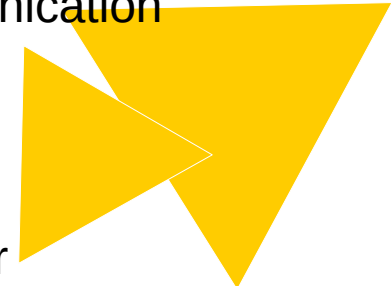
- ▶ Microphone
 - ▷ record audio
- ▶ SMS
 - ▷ read your text messages (SMS or MMS)
- ▶ Wi-Fi connection information
 - ▷ view Wi-Fi connections
- ▶ Location
 - ▷ precise location (GPS and network-based)
 - ▷ approximate location (network-based)



App permissions: Facebook (4)

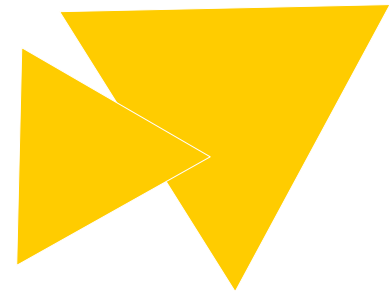
▶ Other

- ▶ download files without notification
- ▶ receive data from Internet
- ▶ adjust your wallpaper size
- ▶ change your audio settings
- ▶ install shortcuts
- ▶ access Bluetooth settings
- ▶ send sticky broadcast
- ▶ toggle sync on and off
- ▶ create accounts and set passwords
- ▶ connect and disconnect from Wi-Fi
- ▶ read sync settings
- ▶ prevent device from sleeping
- ▶ modify system settings
- ▶ change network connectivity
- ▶ run at startup
- ▶ full network access
- ▶ set wallpaper
- ▶ read battery statistics
- ▶ view network connections
- ▶ reorder running apps
- ▶ read Google service configuration
- ▶ pair with Bluetooth devices
- ▶ control Near Field Communication
- ▶ draw over other apps
- ▶ control vibration
- ▶ expand/collapse status bar



Always be wary of apps!

- ▶ „free“ (as in free beer) apps in the App/Play Store often monetize user data and include ads
- ▶ Always ask yourself: Do I really need that app? Does the app need really need certain permissions to function?
- ▶ Restrict permissions of installed apps.
- ▶ Use alternatives, that require less permissions and include less or no trackers.
- ▶ Choose free (as in freedom) software over proprietary apps.





Facebook

7 trackers

54 permissions

Version 243.0.0.47.108 - [see other versions](#)

Created by Facebook

Downloads: 5,000,000,000+

Report created on Oct. 21, 2019, 9:04 a.m. and updated on Nov. 9, 2019, 7:46 p.m.

[See on Google Play](#) >

7 trackers

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

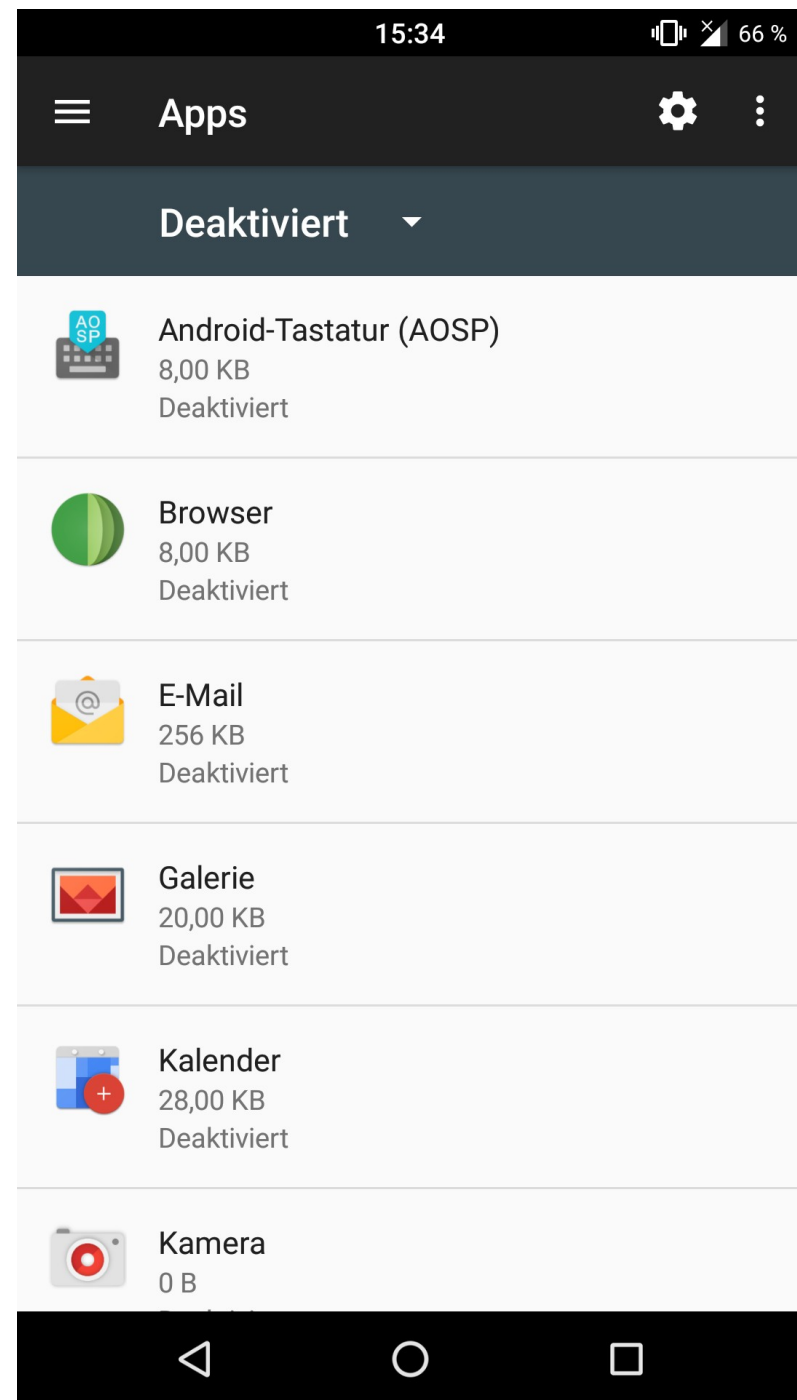
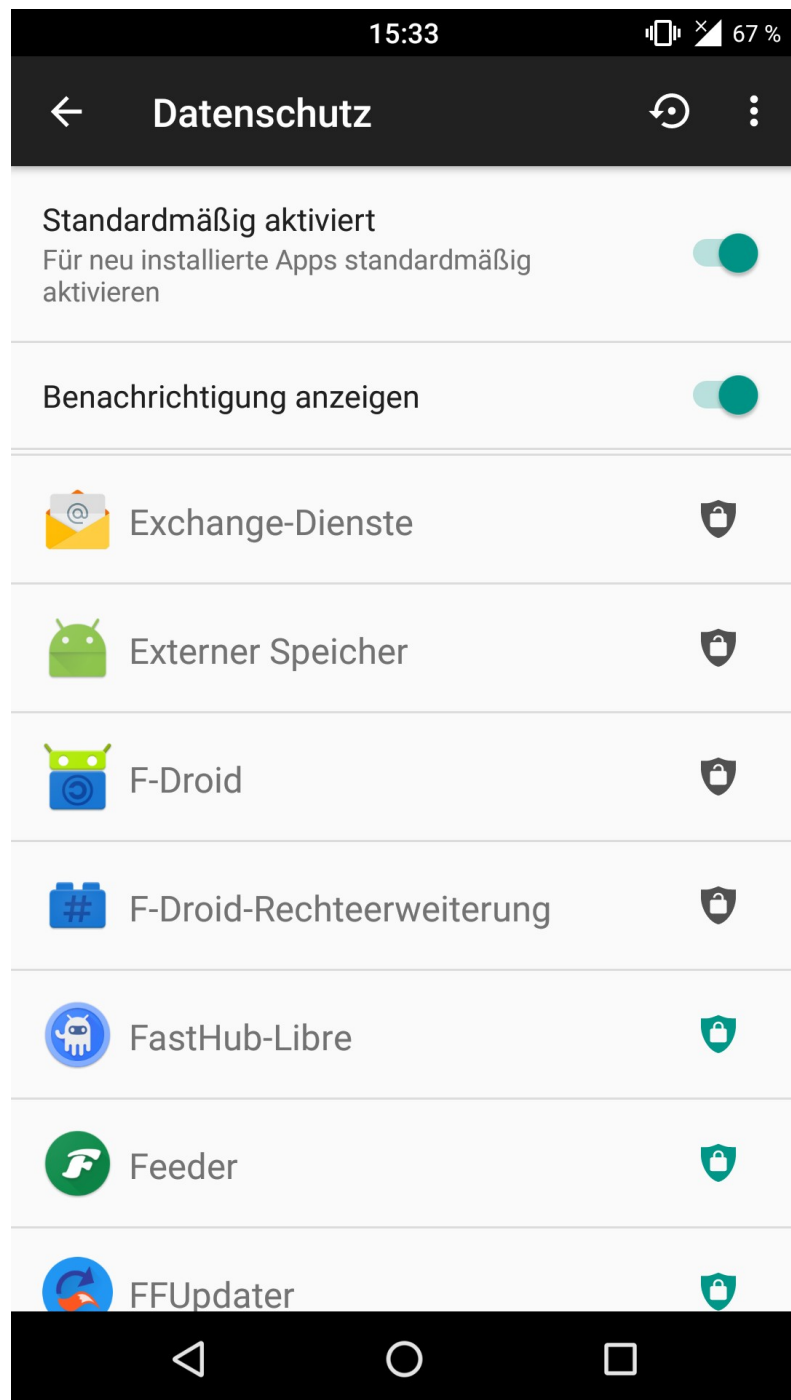
[Facebook Ads](#) >

[Facebook Audience](#) >

[Facebook Notifications](#) >

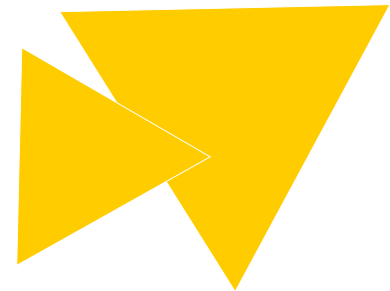
[Facebook Places](#) >





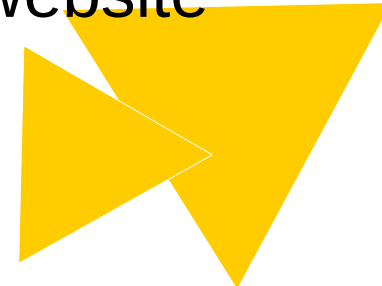
Ungoogle your Android

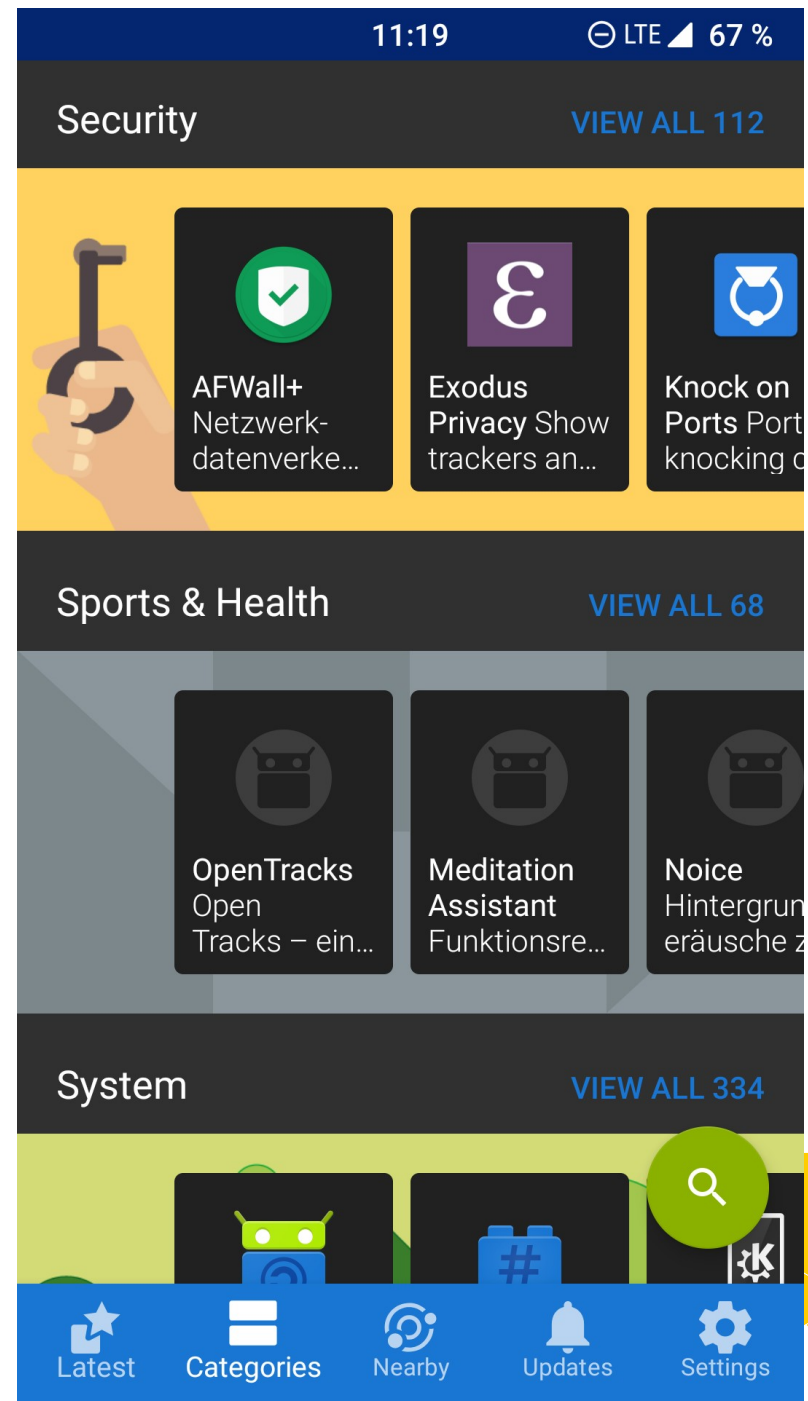
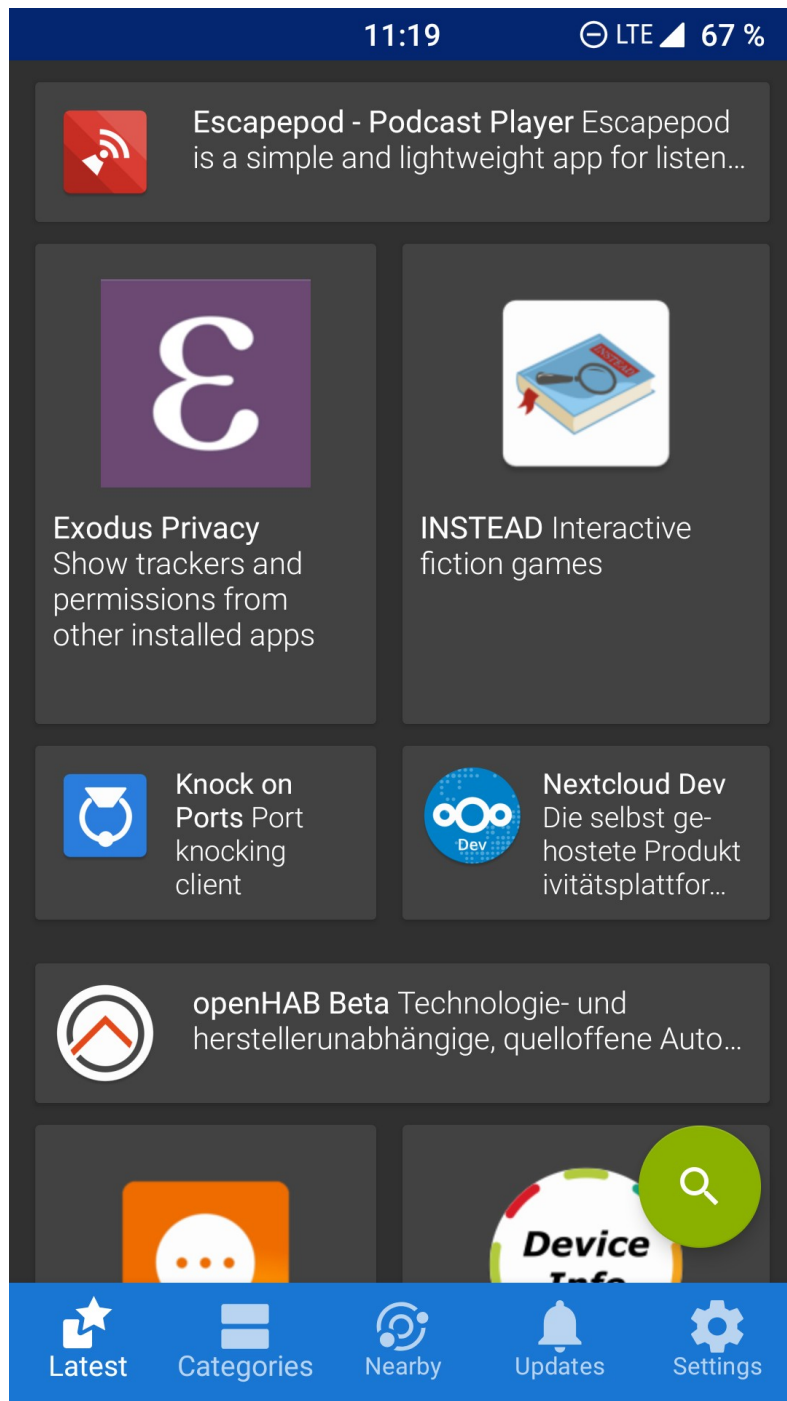
1. Disable or uninstall apps and services by Google
 - Google settings (G+, location, search, Advertising ID and more)
2. Use alternate apps and services
 - Firefox instead of Chrome, Qwant instead of Google search ...
3. Use F-Droid instead of the Play Store
 - Install a Custom ROM without Google Apps
 - e.g. LineageOS, /e/, Replicant



App recommendations: F-Droid

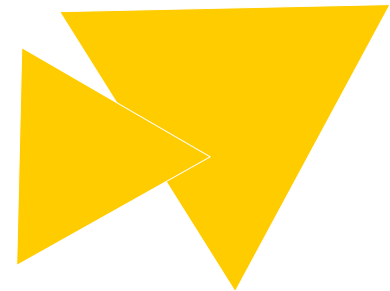
- ▶ App repository as an alternative to the Play Store
 - ▷ <https://f-droid.org/>
- ▶ Exclusively hosts apps under free license
- ▶ No account required
- ▶ New apps for the official F-Droid repository can be submitted by anyone
- ▶ It is possible to use custom repositories.
- ▶ Direct download of apps is possible by using the website





The perfect messenger ...

- ▶ Available for all common operating systems
- ▶ Supports end-to-end encryption
- ▶ Secure encryption algorithm (AES)
- ▶ Decentralized / allows you to host servers
- ▶ Open source (allowing code and security audits)
- ▶ Upload of user data (e.g. contacts) must be voluntary
- ▶ Installation and usage must be possible without dependence on third parties
 - ▷ e.g. without Google Play Store & Play services



... does not exist! (Android)

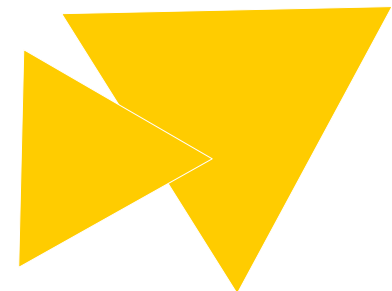
	Signal	Telegram	Threema	WhatsApp	Wire
Free software	yes	Client only	no	no	yes
End-to-end encryption	yes	(yes)	yes	yes	yes
Recent Audit	yes	(yes)	(yes)	no	yes
Contact upload	(no)	(no)	(no)	(no)	(no)
Nicknames (pseudonyms)	no	(yes)	yes	no	yes
Available outside Play Store	yes	yes	yes	yes	yes
Works without Play services	yes	(yes)	yes	no	yes
Install base	medium	large	medium	very large	small

Alternatives to WhatsApp & Co. (1)

▶ **Signal** (Android, iOS)



- ▷ Free Software
- ▷ Trusted end-to-end encryption
- ▷ Supports encrypted text and voice messages, voice and video calls.
- ▷ Phone number mandatory, central structure, based in the US
- ▷ Available in the Play bzw. App Store, Android APK download:
 - <https://signal.org/android/apk/>

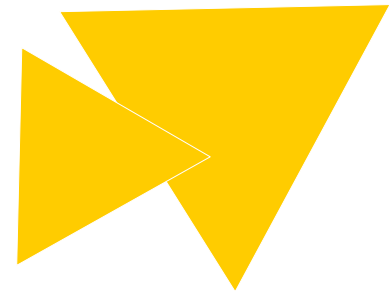


Alternatives to WhatsApp & Co. (2)

▶ **Conversations (Android)** **bzw. ChatSecure (iOS)**



- ▶ Use the open **XMPP protocol** (Jabber), which allows decentral communication
- ▶ Supports end-to-end encrypted chats via OMEMO
- ▶ Available via Play Store / F-Droid (Conversations) and via App Store (ChatSecure)



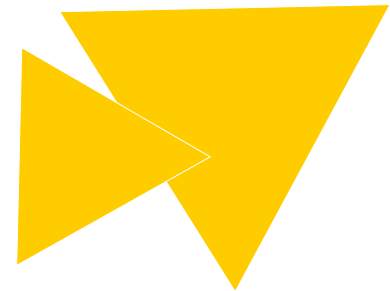
Recommended web browser



▶ **Mozilla Firefox / Fennec F-Droid**

- ▷ Free Software
- ▷ Android version can be customized with add-ons (uBlock Origin, NoScript, HTTPS Everywhere etc.)
- ▷ Configuration mostly similar to desktop version
- ▷ The iOS version is rather limited

▶ **Tor Browser for Android**

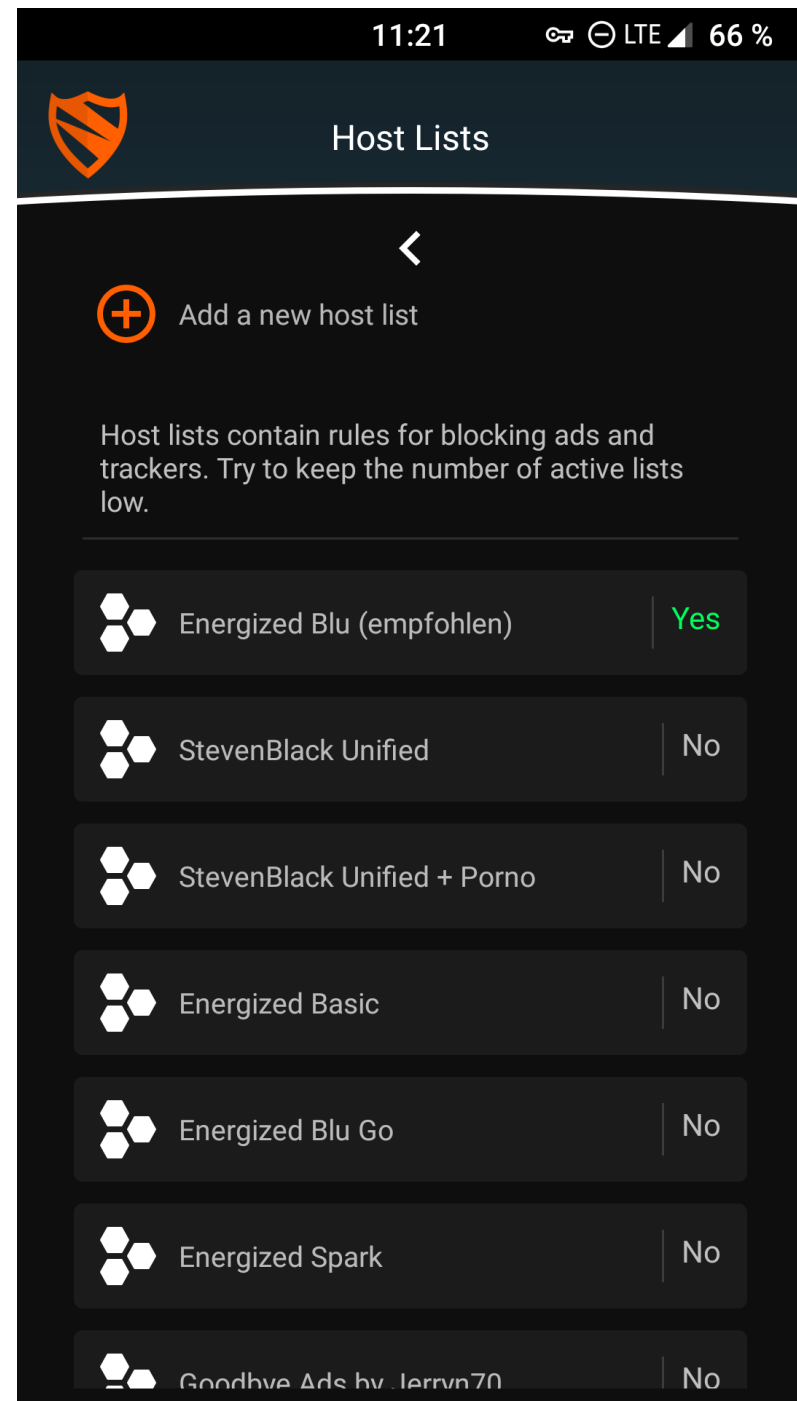
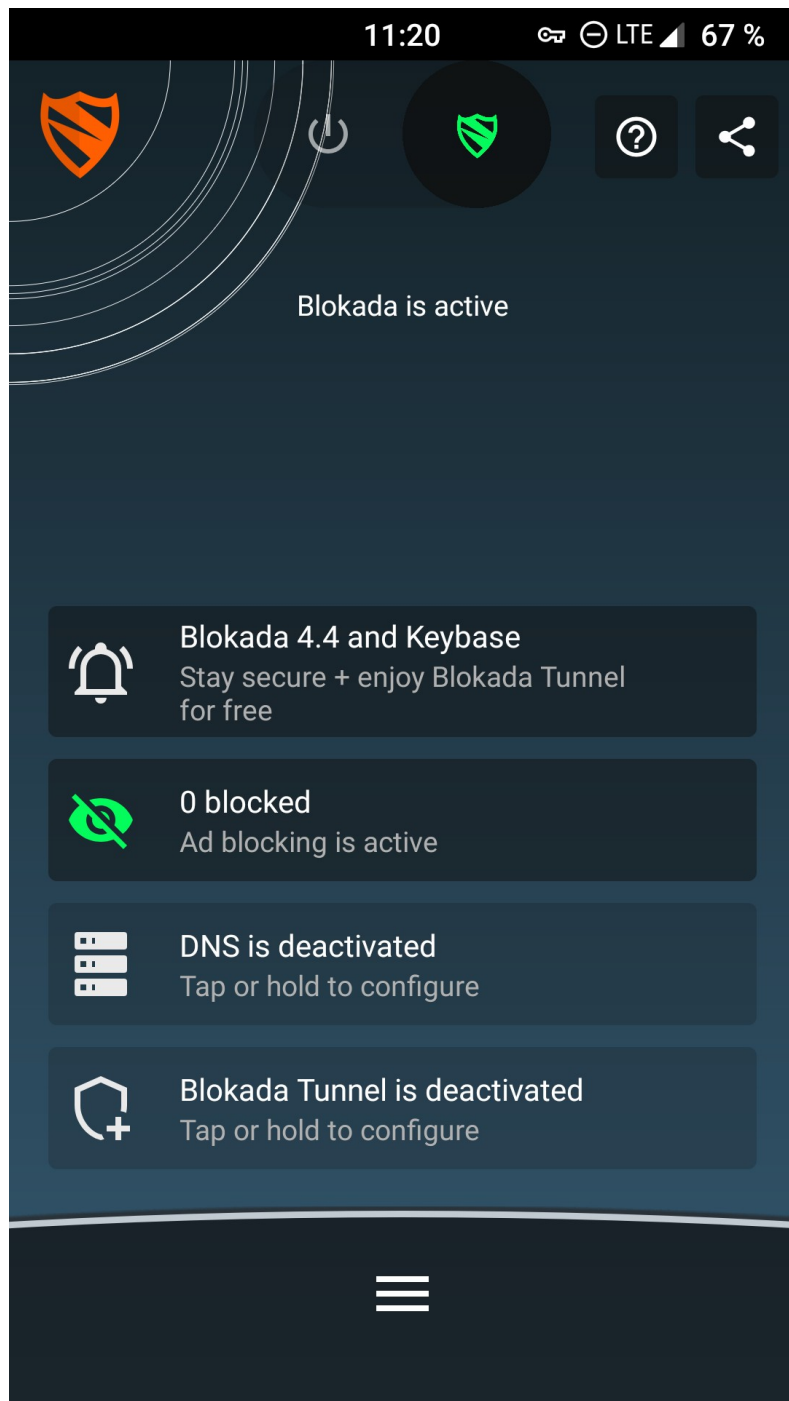


Blokada: blocking of ads and tracking



- ▶ System-wide blocking of ads and tracking by filtering connections via the Android VPN interface
- ▶ Set a custom DNS server
- ▶ Free Software
- ▶ Only available in **F-Droid** or at the official website:
 - ▷ <https://blokada.org/>
- ▶ **WARNING:** Not compatible with Tor Browser or other VPN dependent apps





Recommended email client

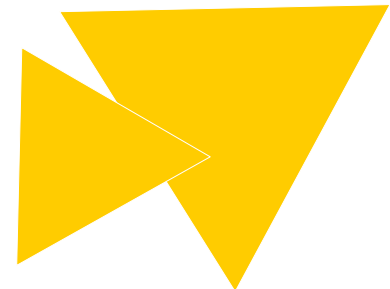
▶ **K-9 Mail**

- ▶ Powerful, free email client
- ▶ Supports IMAP/POP3
- ▶ Can send and receive encrypted mails via PGP/MIME



▶ **OpenKeychain**

- ▶ OpenPGP for Android
- ▶ Includes key management



More recommended apps



▶ **Transportr**

- ▷ Find public transport connections



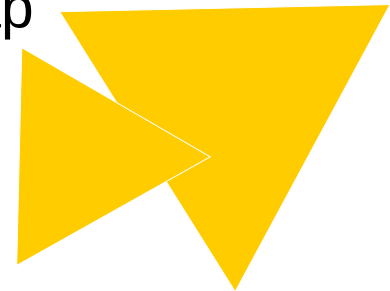
▶ **VLC**

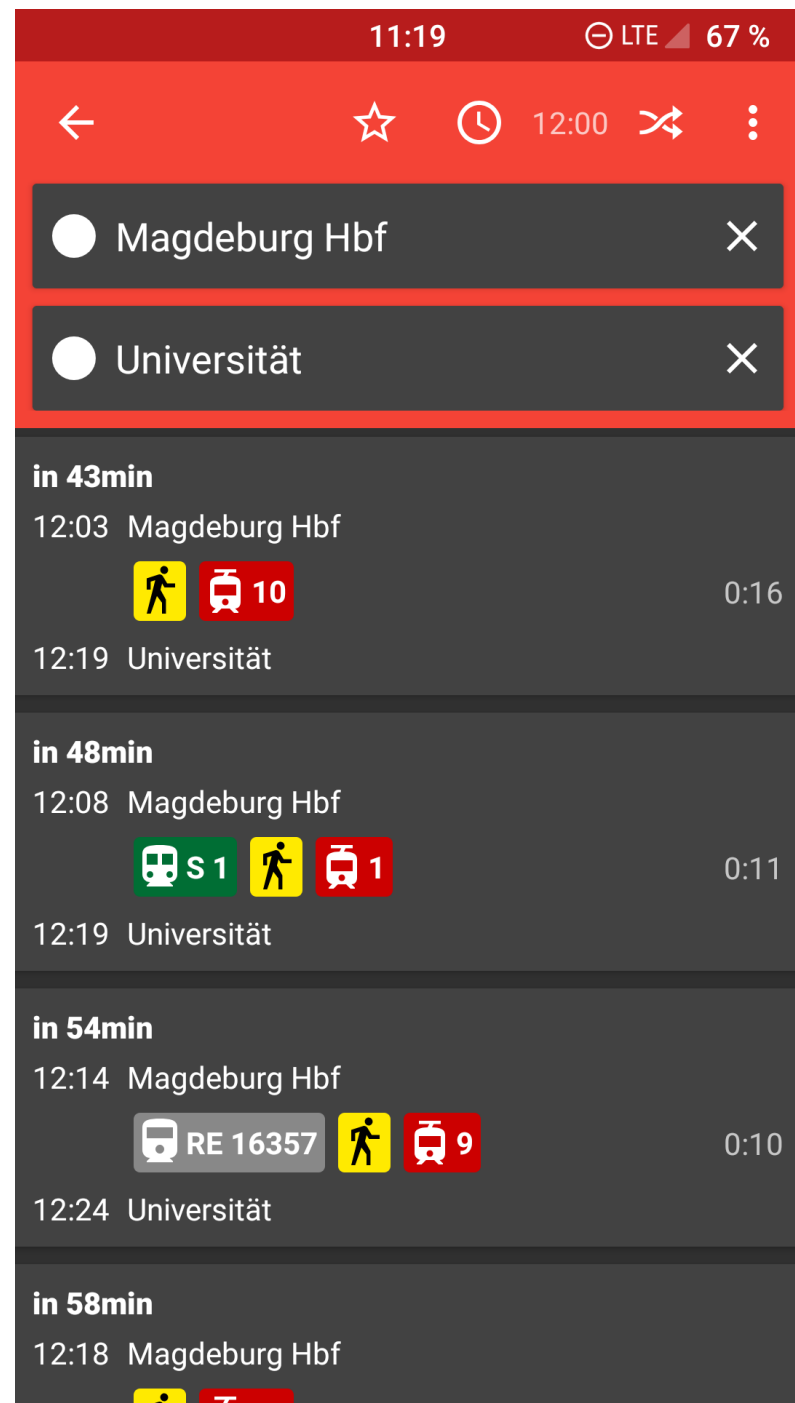
- ▷ Video and audio player



▶ **OsmAnd+**

- ▷ Map and navigation app based on OpenStreetMap
- ▷ Supports offline maps





Recommended projects

▶ **PRISM Break**

▷ <https://prism-break.org/en/>

▶ **CryptoPartys world-wide**

▷ <https://www.cryptoparty.in/>

▶ **Freifunk Magdeburg**

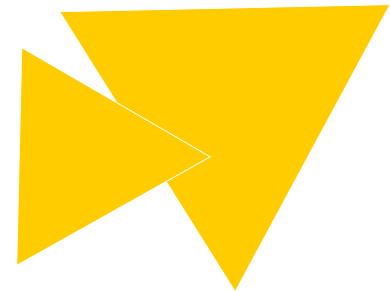
▷ <https://md.freifunk.net/>

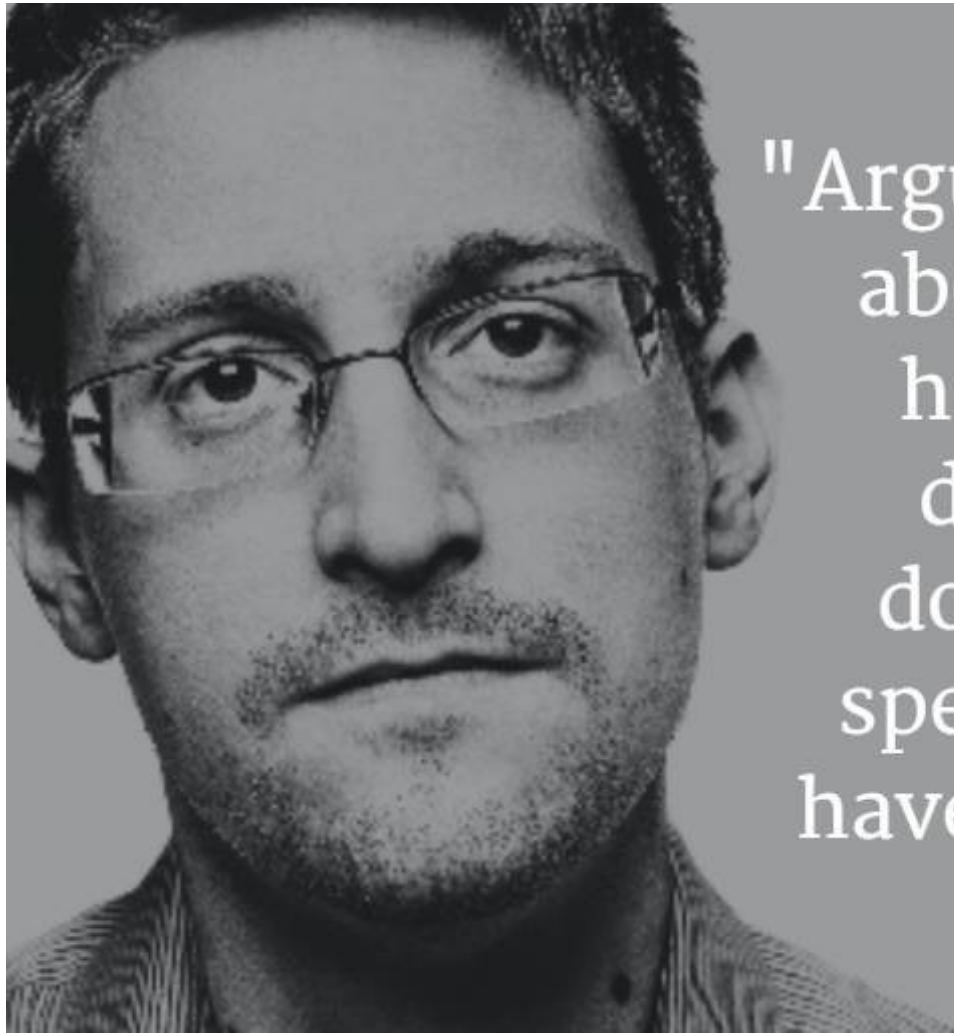
▶ **Surveillance Self-defense by the EFF**

▷ <https://ssd.eff.org>

▶ **Data detox kit by Tactical Tech**

▷ <https://datadetoxkit.org/en/home>





"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."

Thank you for listening.

Let's try that!

