



**Ich habe nichts zu verbergen –
oder doch?**



**Ich will nicht in einer Welt leben,
in der alles, was ich sage, alles was ich mache,
der Name jedes Gesprächspartners,
jeder Ausdruck von Kreativität,
Liebe oder Freundschaft aufgezeichnet wird.**

Edward Snowden

Worum geht es heute?

- Einführung: Warum Datenschutz?
 - Wozu wird getrackt?
- Webtracking
 - Wie wird getrackt?
- Gegenmaßnahmen
 - Browser wählen & einrichten
 - Tor / Tails

Digitalcourage e.V.

- Gemeinnütziger Verein für Datenschutz und Bürgerrechte
 - "Für eine lebenswerte Welt im digitalen Zeitalter"
 - Big Brother Awards (Sa, 8. Juni)
 - Aktionen zu aktuellen Themen
- Digitalcourage-Hochschulgruppe
 - CryptoPartys
 - BackupPartys
 - LinuxInstallPartys (Do, 25. Mai)
 - Regelmäßige Treffen an der Uni

CryptoParty

- Digitale Selbstverteidigung
- Schutz vor Massenüberwachung
- Einsteigerfreundlich
- Öffentlich, nicht-kommerziell, weltweit
- Von AnwenderInnen für AnwenderInnen
 - Mach mit und werde Teil der CryptoParty-Bewegung

- <https://cryptoparty.in>



Warum Datenschutz?

Zwei einführende Beispiele

1. Schöne neue Welt – „schöne“ neue (techn.) Möglichkeiten:

- „SHORE® – Neue Wege in der Gesichtsanalyse“ (Fraunhofer IIS)

Zwei einführende Beispiele

2. Datenhandel und -verwertung (Doku. *Der gläserne Deutsche*)

- AZ Direkt
- Facebook
- ...

Zwei einführende Beispiele

- *Facebook*, siehe:

<https://netzpolitik.org/2016/98-daten-die-facebook-ueber-dich-weiss-und-nutzt-um-werbung-auf-dich-zuzuschneiden/>

Auszug:

- Ort; Alter; Geschlecht; Bildungsniveau; Einkommen und Eigenkapital;
- Hausbesitz und Hauswert; Grundstücksgröße; Hausgröße in Quadratmetern;
- Nutzer, die frisch verheiratet sind; Beziehungsstatus;
- Nutzer, die planen, ein Auto zu kaufen (welche Art/Marke, und wann);
- Betriebssystem, Emailanbieter, Art der Internetverbindung;
- Nutzer, die Browserspiele spielen;
- Nutzer, die eine Facebook-Veranstaltung erstellt haben;
- Anzahl der Kredite;
- Nutzer, die aktiv eine Kreditkarte benutzen;

- Arten von Kleidung, die der Haushalt des Nutzers kauft;
- Die Zeit im Jahr, in der der Haushalt des Nutzers am meisten einkauft;
- **Nutzer, die „sehr viel“ Bier, Wein oder Spirituosen kaufen;**
- **Nutzer, die Medikamente gegen Allergien und Schnupfen/Grippe, Schmerzmittel und andere nicht-verschreibungspflichtige Arzneimittel einkaufen;**
- **Nutzer, die „empfindlich“ [sind] für [Werbung zu] Online-Autoversicherungen, Hochschulbildung oder Hypotheken, Prepaid-Debitkarten und Satellitenfernsehen;**
- Wie lange der Nutzer sein Haus bereits bewohnt;
- Nutzer, die wahrscheinlich bald umziehen;
- ...

Privatsphäre als persönlicher Bereich



Privatsphäre

„Privat ist etwas genau dann, wenn man den Zugang dazu kontrollieren kann.“ (Rössler, 2001)

Privatsphäre ist wichtig für das **Individuum** und für die **Gesellschaft**, weil ...

Rössler, Beate: Der Wert des Privaten, Frankfurt: Suhrkamp, 2001

Privatsphäre

Wichtig für das **Individuum**:

- „The right to be left alone.“
- Freie Entfaltung der Persönlichkeit
- Kontrolle über die Folgen des eigenen Handelns
- Selbstbestimmung (wer weiß was von mir)
- Schutz vor Kritik und Diskriminierung
- Sicherheit (Passwörter, Eigentum, ...)
- Freiheit
- Intimität?

Privatsphäre

Wichtig für die **Gesellschaft**:

- Essentiell für Demokratie und Rechtsstaat:
 - Verschwiegenheitspflicht (Medizin, Recht, Beratung, ...)
 - Journalismus (Quellenschutz)
 - Abwehrrecht gegen die Staatsmacht
- Soziale Rollen (unterschiedliches Verhalten)
- Fortschritt ermöglichen (Opposition zulassen)
 - Sobald Offenlegung sich zur sozialen Norm entwickelt, wird das Gegenteil zum Stigma

Privatsphäre

- Analog

- Privatsphäre selbstverständlich akzeptiert
- Einbrüche in Privates meist erkennbar
- Gesetze zum Schutz der Privatsphäre
 - Unverletzlichkeit der Wohnung
 - Briefgeheimnis
 - Freie Entfaltung der Persönlichkeit

- Digital

- Neuer Wirtschaftsraum
- Neue technische Mechanismen / Möglichkeiten
- Intransparente Datenerhebung und -nutzung
- Technisches Verständnis häufig notwendig
- Datenschutzgesetze nicht zeitgemäß, #neuland

Juristischer Ansatz

*„Datenschutz beobachtet, beurteilt und gestaltet die asymmetrischen Machtbeziehungen zwischen **mächtigen Organisationen (Risikogebnern)** und im Grundsatz selbstständig agierenden **Personen (Risikonehmer)**.“*

Als Schutz des Individuums!

Digitale Identität



Google-Dienste

- Was für Dienste bietet Google an?

Google-Dienste

Google Suchmaschine

- Marktanteil weltweit ca. 90%
- Als Standard vorinstalliert
 - Chrome, Firefox
 - Android (ist Google)
- Google Sprachsuche

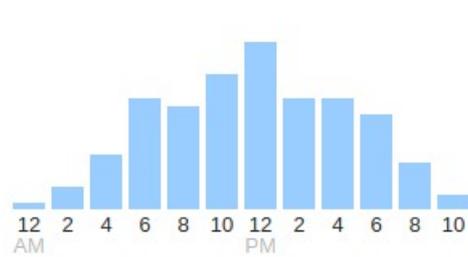
Erfasste Daten

- Suchbegriffe (Search History)
 - eingegeben, gesehen, angeklickt
- IP-Adresse
- Sprache
- Datum, Uhrzeit
- Gerät, Betriebssystem, Browser
- Standort (GPS oder Browser)
 - <https://myactivity.google.com/>

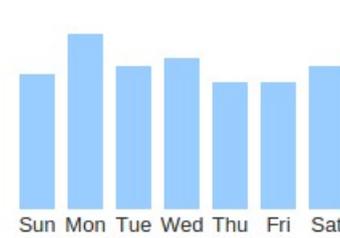
History

Only you can see your history

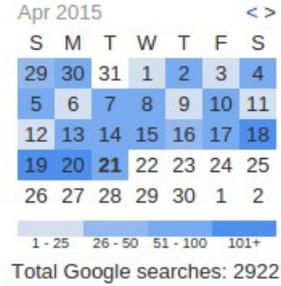
Hourly search activity



Daily search activity



Activity



[Show more trends >>](#)



Remove items

Older >

[View additional Web & App Activity](#)

Today

- Searched for [site:tech-recipes.com cookies hosts](#) 6:53pm
[How Do I Block Ad Cookies and Data Brokers... - tech-recipes.com](#) 6:54pm
- Searched for [site:tech-recipes.com tracking cookies](#) 6:53pm
[How to Use Chrome Incognito Mode | a... - tech-recipes.com](#) 6:53pm
- Searched for [chrome show cookies](#) 6:46pm
[4 Ways to View Cookies - wikiHow - wikihow.com](#) 6:46pm
- Searched for [login to chrome](#) 6:36pm
[Sign in - Google Accounts - google.com](#) 6:36pm
- Searched for [site:tech-recipes.com google search history](#) 6:34pm
[Google History: How to enable, disable,... - tech-recipes.com](#) 6:34pm
- Searched for [604800/60/60/24](#) 5:48pm
- Searched for [604800/60/60/24 or 21](#) 5:48pm



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

Constanze Kurz, Chaos Computer Club

Folgen

- Sehr viel Wissen über die Nutzer
 - Interessen, Krankheiten, sexuelle Vorlieben, Bewegungsprofil...
- Zusammenführung von Daten verschiedener Quellen
 - Suche, YouTube, Gmail, Analytics, AdWords, Android...
- Individualisierung der Suchergebnisse (Filter-Bubble)
- Big Data
 - Suchtrends (regional, weltweit)
- Datenhandel
 - Werbung, Kreditwürdigkeit, Versicherungen..

Google Analytics

- Einbindung auf der Webseite
- Statistiken für die Betreiber der Webseite
- Tracking der Besucher beim Seitenaufruf
 - IP-Adresse, Sprache, Land
 - Datum, Uhrzeit
 - Gerät, Betriebssystem, Browser
 - Bildschirmauflösung
 - Referer (von welcher Webseite gekommen)

+ Add Widget | Share | Email | Export

Customize Dashboard | Delete Dashboard

All Sessions
100.00%

+ Add Segment

Unique visitors

281,023

% of Total: 100.00% (281,023)



New users

60.72%

Site Avg: 60.72% (0.00%)



Unique smartphone/tablet visitors

23,863

% of Total: 8.49% (280,992)



Top 5 Country Origin

Country / Territory	Users	% New Sessions
United States	79,644	59.81%
United Kingdom	23,652	58.24%
India	17,322	68.59%
Netherlands	14,049	51.75%
Canada	11,392	60.10%

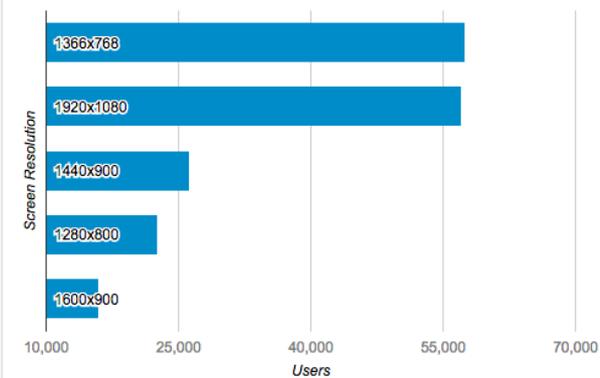
Visitors' favorite browsers

Browser	Users	Bounce Rate
Chrome	161,398	70.61%
Firefox	68,844	70.86%
Safari	29,945	72.77%
Internet Explorer	12,907	70.23%
Safari (in-app)	2,906	89.06%
Opera	2,318	72.79%
Android Browser	1,781	79.31%
Opera Mini	765	73.64%
YaBrowser	257	77.47%
UC Browser	250	77.53%

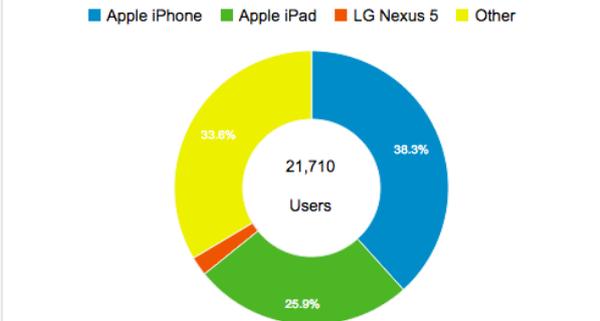
Unique visitors



Top 5 screen resolutions



Top 3 mobile devices for users



% Sessions with Search

1.03%

Site Avg: 1.03% (0.00%)



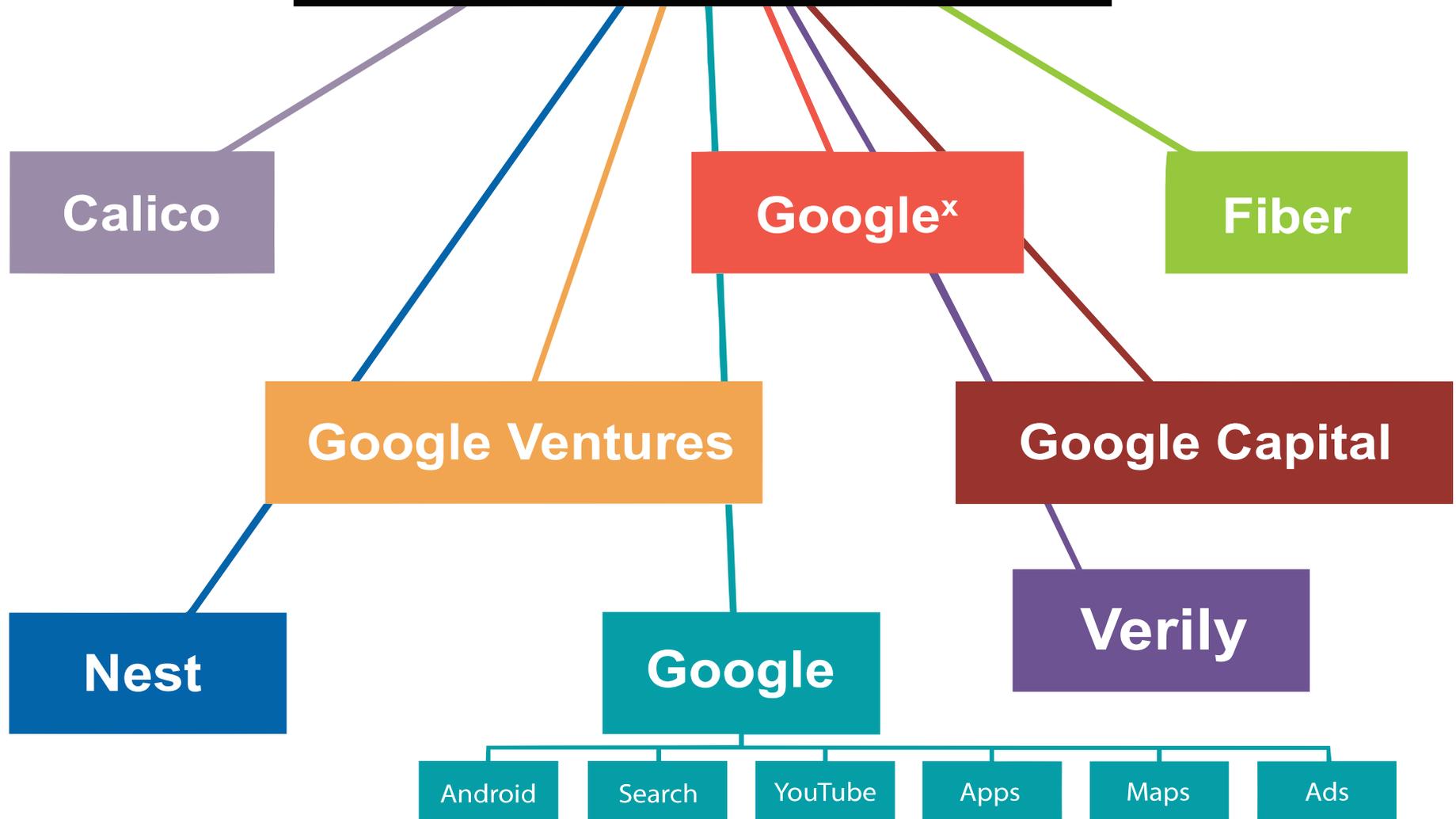
Sessions and Bounce Rate by Source / Medium

Source / Medium	Sessions	Bounce Rate
wordpress-seo-metabox / inline-help	25,687	77.07%
wordpress-seo-config / banner	18,568	69.65%
gawp-config / kb-link	8,087	69.40%
gawp-config / textlink	6,826	74.48%
wpseo_dashboard / wpseo_tour	5,314	75.05%
gawp-config / banner	3,408	74.94%
newsletter-10-october-2014 / newsletter	3,311	61.70%
newsletter-23-october-2014 / newsletter	3,308	58.40%
newsletter-3-october-2014 / newsletter	3,099	70.41%
wpadmin / plugin	3,063	64.38%

Sessions and Bounce Rate by Campaign

Campaign	Sessions	Bounce Rate
focus-keyword	22,627	76.13%
wpgapplugin	17,878	70.60%
extension-page-banners	13,679	71.69%
tour	6,750	75.17%
wpseoplugin	4,678	67.61%
newsletter-10-october-2014	3,311	61.70%
newsletter-23-october-2014	3,307	58.39%
snippet-preview	3,133	84.26%
newsletter-3-october-2014	3,095	70.44%
website-review-banner	3,091	73.34%

Alphabet



Facebook

- „Kostenlos“
- Datenschutzeinstellungen werden immer schwieriger
- Klarnamenpflicht
- Rechte an den Daten
- Intransparenz bei der Weitergabe
- Lock-In (kein Profil-Export)
- <https://dayssincelastfacebookscandal.com/>

Schön zusammengefasst von Alexander Lehmann (für X3)

- Video (<https://vimeo.com/16203416>)

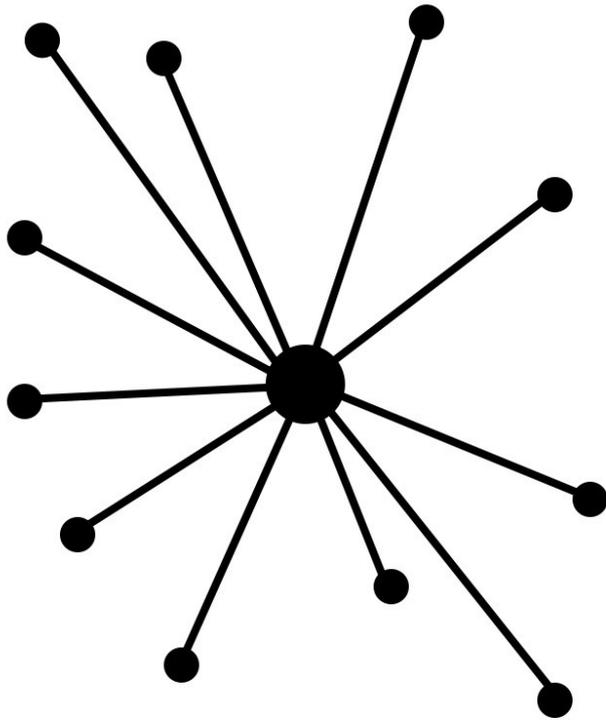
Datenwirtschaft

- „Kostenlose“ Angebote
 - Daten sind eine neue Währung
 - Datenhändler kaufen Profile und verkaufen sie an die Werbeindustrie, Versicherungen, Schufa, etc.
- Geschlossene Systeme
 - Proprietäre Software
 - Keine offenen Schnittstellen
- Big Data
 - Zusammenführung, Analyse und Auswertung großer Datenmengen

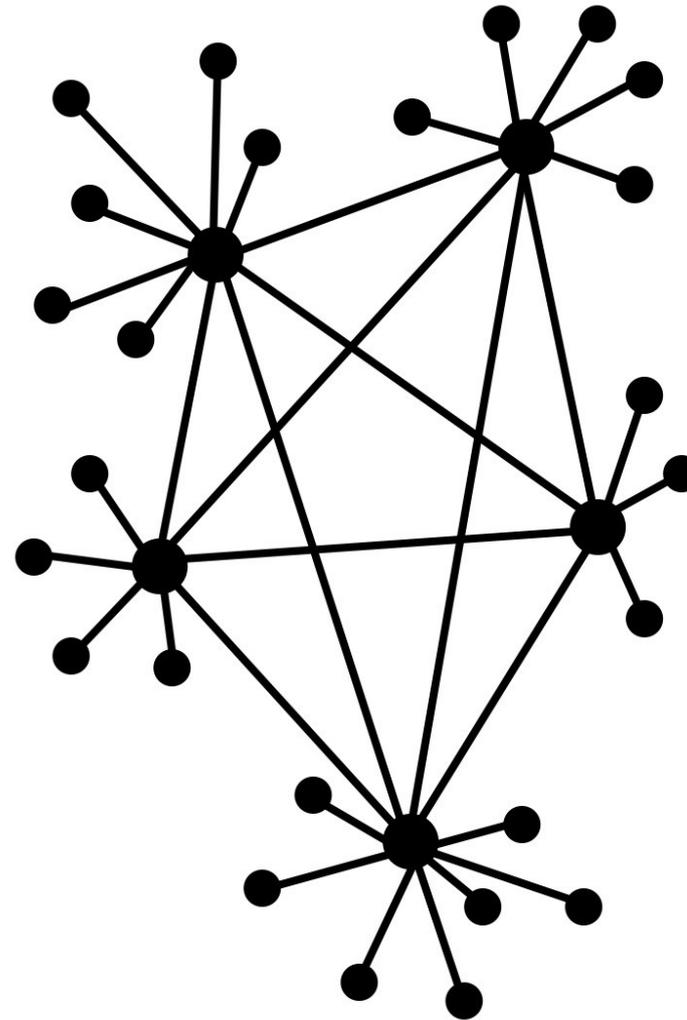
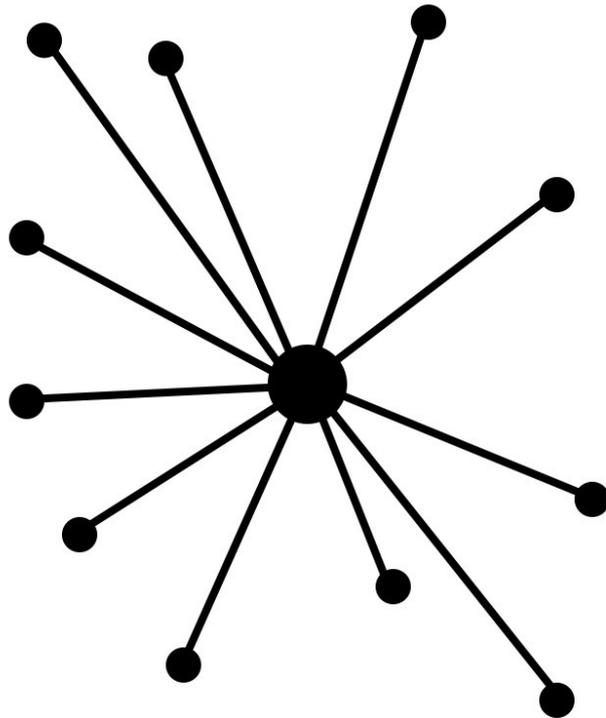
Datenwirtschaft

- Sicherheit
 - Bedeutet Aufwand = Kosten
- Datenschutz
 - Weniger Daten für das Unternehmen
 - Weniger Rohmaterial zum Analysieren und Verkaufen
 - Privatsphäre "überholt"?
- DSGVO

Zentral vs. Dezentral



Zentral vs. Dezentral



Begriff: Metadaten

- Inhalt
- Metadaten (Nachricht)
 - Absender, Empfänger
 - Datum, Uhrzeit
 - IP-Adresse / Mobilfunknetz
- Metadaten (Foto)
 - Auflösung
 - Blende, Belichtungszeit
 - GPS Koordinaten

Lieber Max,

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



Viele Grüße
Leah

Begriff: Metadaten

In der Telekommunikation häufig *Verbindungsdaten* genannt.

- Kleine Datenmenge
- Leicht zu analysieren (im Gegensatz zu Inhalt)
- Schwierig zu verschlüsseln
 - da notwendig um die Kommunikation zu ermöglichen

**Metadaten eignen sich perfekt zur Datenanalyse
und Massenüberwachung!**



We Kill People Based on Metadata

General Michael Hayden, Ex-Chef von NSA und CIA

Datenschutz = Menschenrecht



Foto: Gerichtshof der Europäischen Union

Charta der Grundrechte der
Europäischen Union

Art. 8

Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf
Schutz der sie betreffenden
personenbezogenen Daten.

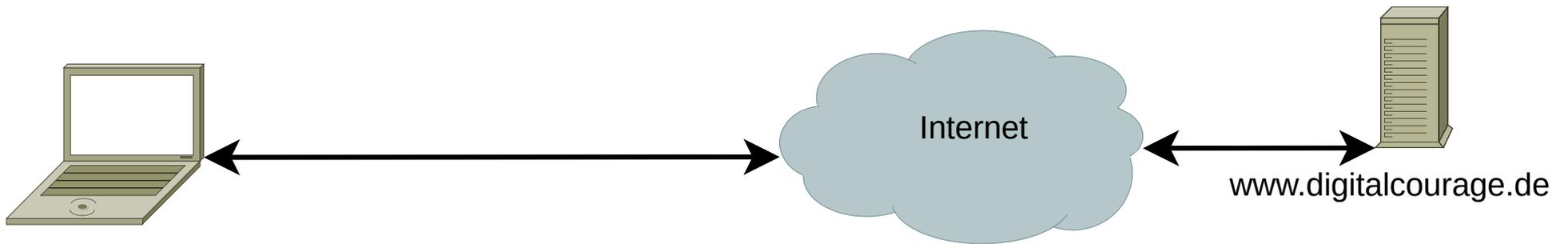


Hör-/Leseempfehlungen

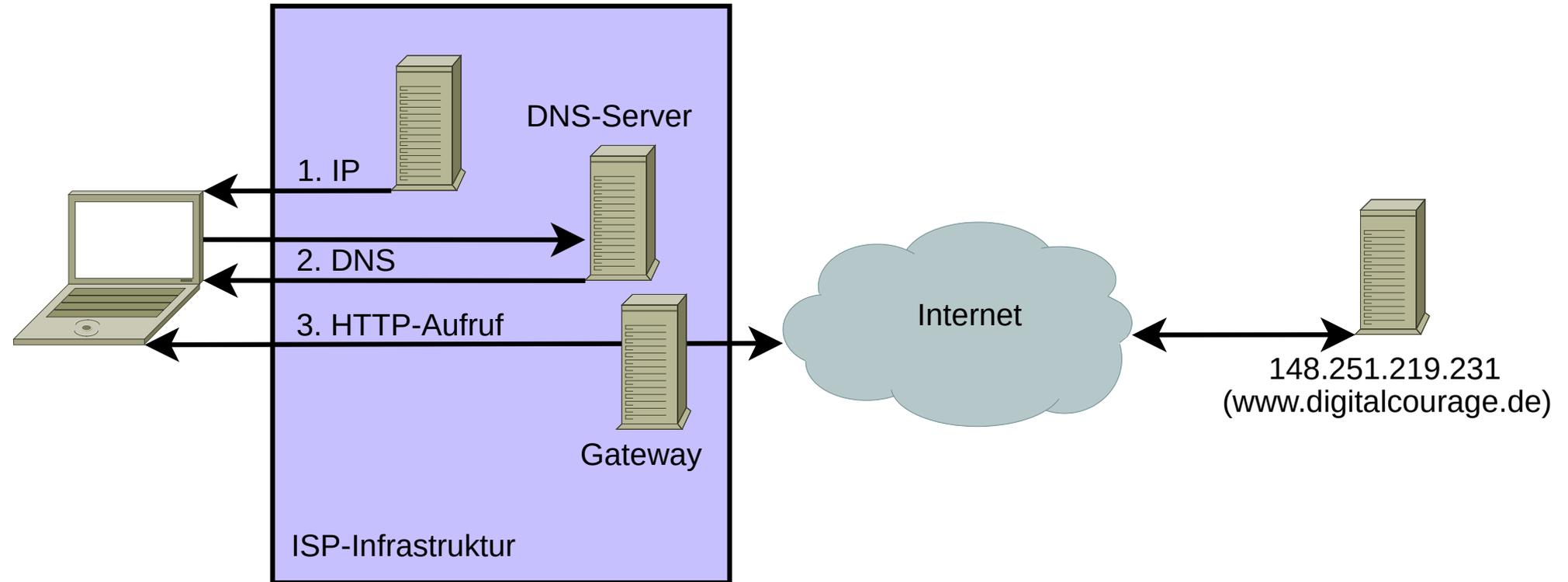
- <https://netzpolitik.org>
- Buch: "Die globale Überwachung" (Glenn Greenwald)
- Buch: "Was Google wirklich will" (Thomas Schulz)
- Videos: <http://www.alexanderlehmann.net/>
- Denkangebot Podcast (Katharina Nocun)
 - Folge 4 (5. Mai 2019): Nix zu verbergen
 - <https://www.denkangebot.org/allgemein/da004-nix-zu-verbergen/>

Webtracking

Wie funktioniert das Internet?



Und technisch?



Wie schrecklich ist die Web-Realität?

- Beispiel: www.spiegel.de (Standard-Firefox)

... so schrecklich!

- Beispiel: www.spiegel.de (Standard-Firefox)
- 413-440 (nach 20s) HTTP-GETs an folgende Domains...
- Ablida.net, adition.com, adsrvr.org, atdmt.com, demdex.net, doubleclick.net, exactag.com, google.com, ioam.de, parsely.com, spiegel.de, t4ft.de, theadex.com, twiago.com, xplosion.de, yieldlab.net (ohne Subdomains)
- 8-10 MB; 59 Cookies von 24 Servern
- Ladezeit ca. 15-30 Sek. + Nachladen ohne Interaktion

Einfach selber testen mit Webbkoll

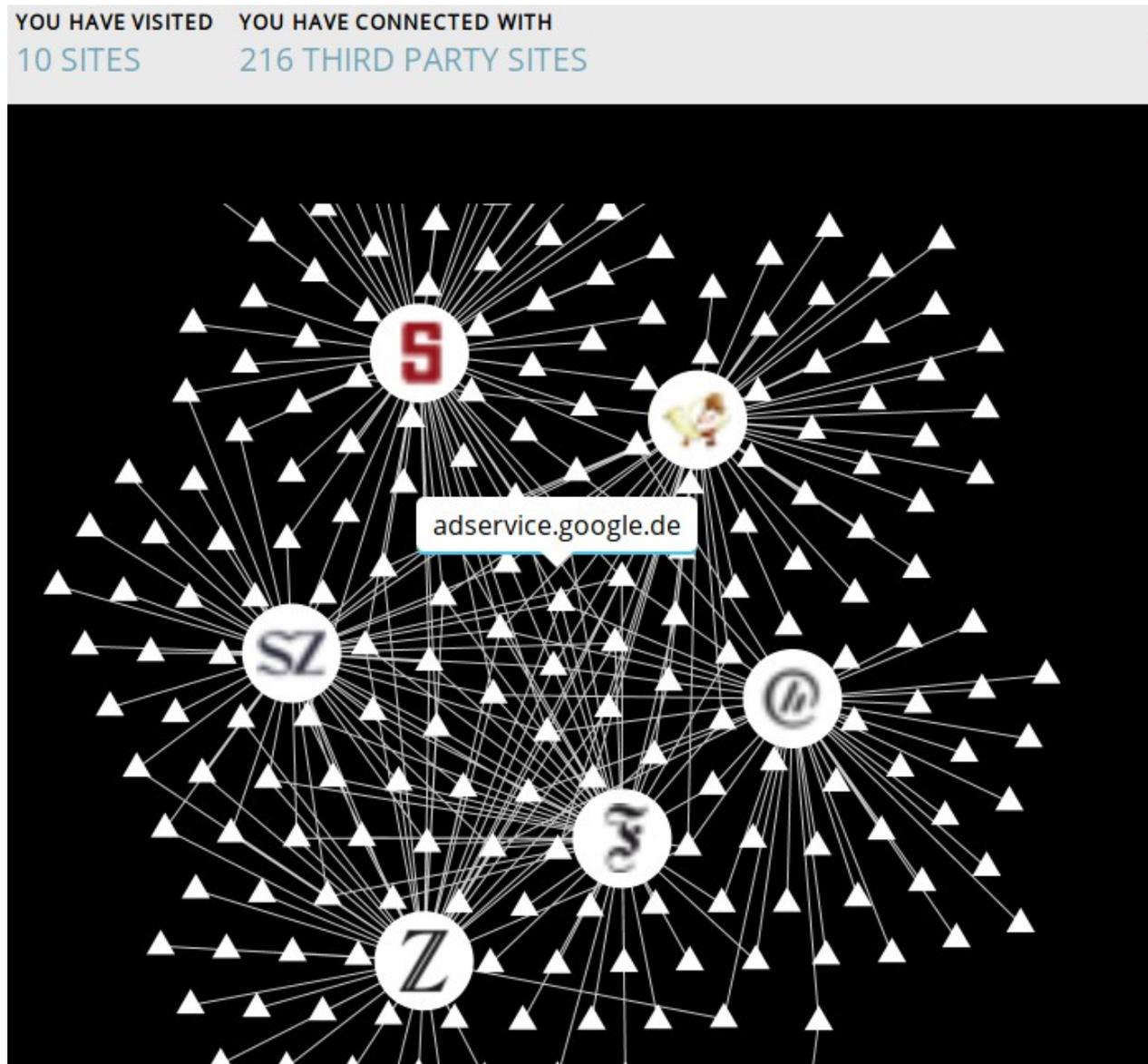


The screenshot shows the webbkoll interface for the website www.spiegel.de. The navigation bar includes the logo, the name 'webbkoll | dataskydd.net', and links for 'Neuigkeiten', 'Über', 'FAQ', and 'Deutsch'. The main heading is 'Ergebnisse für www.spiegel.de'. Below this, several security and privacy metrics are listed with their status:

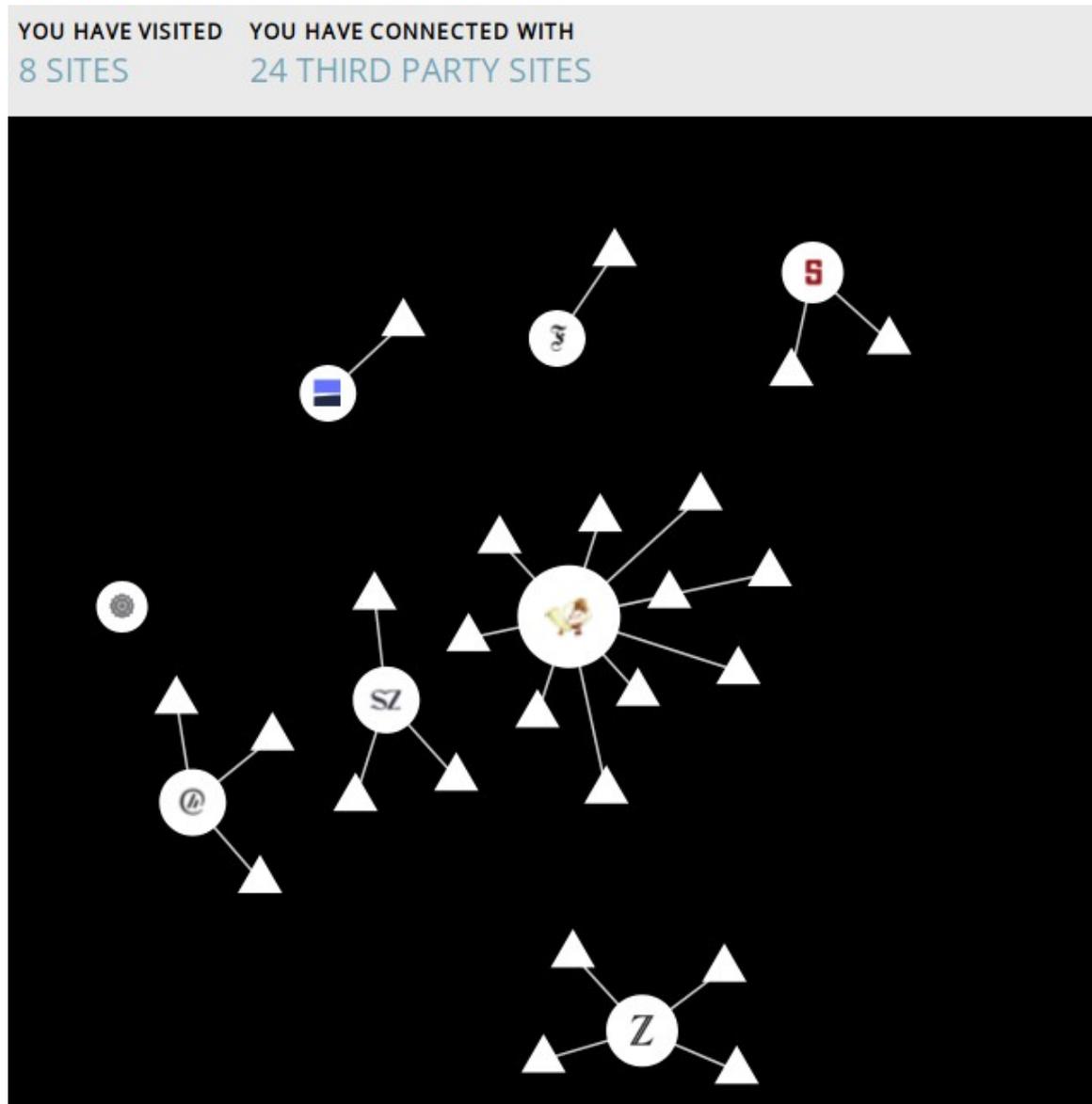
HTTPS als Voreinstellung:	✓ Ja
Content Security Policy:	✗ fehlt
Referrer Policy:	✗ Referrers werden übermittelt
Cookies:	52 (30 First-Party; 22 Third-Party)
Drittanfragen (Third-Party):	223 Anfragen zu 60 eindeutigen Hosts
Serverstandort:	 Deutschland — 128.65.210.181 Nachschlagen

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

Analyse in Firefox mit Lightbeam



Analyse in Firefox mit Lightbeam



Wie wollen wir heute Surfen?

- Sicheres Surfen
 - Schutz des eigenen Geräts/Browsers vor Angriffen aus dem Internet.
- Spurenarmes Surfen
 - Tracking- und Auswertungsmechanismen aushebeln
- Anonymes Surfen
 - Schutz der eigenen Identität und Schutz vor Repressionen

Wie wollen wir heute Surfen?

- **Sicheres Surfen**
 - Schutz des eigenen Geräts/Browsers vor Angriffen aus dem Internet.
- **Spurenarmes Surfen**
 - Tracking- und Auswertungsmechanismen aushebeln
- **Anonymes Surfen**
 - Schutz der eigenen Identität und Schutz vor Repressionen

Wie kann ein Webserver mich identifizieren und verfolgen (Tracking)?

- Cookies
 - Kleine Textdateien, die die aufgerufene Webseite im Browser speichern und wieder abrufen kann.
- Passive Merkmale:
 - IP-Adresse, Sprache, Browser, Betriebssystem
- Aktive Merkmale (JavaScript, Flash, Java, h264, ...)
 - Schriftarten, Browser-Add-ons, Bildschirmauflösung uvm.
- Fingerprinting: Eindeutiger Browser-Fingerabdruck:
 - <https://panopticklick.eff.org>

PANOPTICCLICK^{3.0}

Is your browser safe against tracking?

When you visit a website, online trackers and the site itself may be able to identify you – even if you’ve installed software to protect yourself. It’s possible to configure your browser to thwart tracking, but many people don’t know how.

Panopticlick will analyze how well your browser and add-ons protect you against online tracking techniques. We’ll also see if your system is uniquely configured—and thus identifiable—even if you are using privacy-protective software. However, we only do so with your explicit consent, through the TEST ME button below.

TEST ME

Test with a real tracking company [what's this?](#)

Only **anonymous data** will be collected through this site.

Panopticlick is a research project of the Electronic Frontier Foundation. EFF operates Panopticlick in the United States, which may not provide as much privacy protection as your home country. Panopticlick is part of an effort to illustrate the problem with tracking techniques, and help get stronger privacy protections for everyone. [Learn more.](#)

Test	Result
Is your browser blocking tracking ads?	X no
Is your browser blocking invisible trackers?	X no
Does your browser unblock 3rd parties that promise to honor Do Not Track ?	X no
Does your browser protect from fingerprinting ?	X your browser has a unique fingerprint

Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticlick does not measure all forms of tracking and protection.

Your browser fingerprint **appears to be unique** among the 199,566 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.61 bits of identifying information**.

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
User Agent	5.72	52.63	Mozilla/5.0 (X11; Linux x86_64; rv:66.0) Gecko/20100101 Firefox/66.0
HTTP_ACCEPT Headers	1.75	3.37	text/html, */*; q=0.01 gzip, deflate, br en-US,en;q=0.5
Browser Plugin Details	0.93	1.9	undefined
Time Zone	2.41	5.3	-120
Screen Size and Color Depth	5.73	52.9	1600x900x24
System Fonts	7.3	157.24	Arial, Bitstream Vera Sans Mono, Bookman Old Style, Century Schoolbook, Courier, Courier New, Helvetica, Palatino, Palatino Linotype, Times, Times New Roman, Wingdings 2, Wingdings 3 (via javascript)
Are Cookies Enabled?	0.28	1.22	Yes
Limited supercookie test	0.41	1.33	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	7.81	224.71	5143f917309e471eec7352a63d6e7524
Hash of WebGL fingerprint	8.84	458.71	8689cb4b28cb3c4b7cf8a74839409fea
DNT Header Enabled?	1.26	2.4	False
Language	1.01	2.01	en-US
Platform	2.91	7.52	Linux x86_64
Touch Support	0.77	1.71	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false

Weitere Trackingmechanismen

- EverCookies
 - Cookies werden durch lokal gespeicherte Informationen wiederhergestellt
- URL-Parameter
 - Informationen werden als Teil der URL gesendet
- Tracking-Pixel
 - Meist unsichtbare 1x1 Pixel große Grafiken, um z.B. Aufrufe zu erfassen
- Referrer
 - Herkunftsseite wird beim Wechsel auf eine andere Website übertragen

Wahl des Browsers: Mozilla Firefox



- Freie Software
- Mozilla-Stiftung
- Lässt sich am besten datenschutzfreundlich einrichten
- Die einzige Konkurrenz zu Browsern auf Basis von Google Chrome/Chromium
- Auch unter Android mit Add-ons nutzbar

Wie kann man Tracking abwehren? (1)

- Browser-Einstellungen
 - Do-not-track-option
 - Benutzerdefinierte Chronik, Cookies für Drittanbieter deaktivieren
 - JavaScript abschalten, wenn möglich
 - Siehe Handout
- Suchmaschinen
 - Startpage.com, MetaGer.de, Searx.me etc. (im Gegensatz zu Google auch keine individualisierten Ergebnisse)
- Browser-Add-ons!

Wie kann man Tracking abwehren? (2)

- Cookies:
 - Browser-Einstellungen, Add-ons, Löschen der Chronik, privater Modus
- Fingerprinting:
 - JavaScript deaktivieren, NoScript, diverse Add-ons
 - Tor-Browser

Wie kann man Tracking abwehren? (3)

- EverCookies:
 - Add-ons, um Websitedaten zu isolieren
 - Manuelles Löschen der Chronik
- URL-Parameter:
 - URLs/Links vor Aufruf händisch kürzen
 - Add-on
- Tracking Pixel:
 - Werbe-/Trackingblocker (Add-on)
- Referrer:
 - Spezielle Browser-Einstellungen, Add-on

Firefox-Add-ons

- Tracker und Werbung blocken: **uBlock Origin**
- Aktive Inhalte blocken: **NoScript**
- Cookies automatisch löschen: **Cookie AutoDelete**
- Webseiten immer verschlüsseln: **HTTPS Everywhere**
 - Schützt zwar nicht gegen Tracking, erhöht aber die Sicherheit. :)

uBlock Origin: mehr als nur ein Werbeblocker



- Blockt neben Werbung auch andere trackende Elemente.
- Viele Filterlisten verfügbar.
 - Blockt so auch u.a. Malware-Seiten, Social-Media-Elemente, Cookie-Warnungen, Tracking-Pixel usw.. :)

+ Werbung (1/4)

[EasyList](#) 🏠 89.255 benutzt aus 89.479 ⓘ

+ Privatsphäre (1/3)

[EasyPrivacy](#) 🏠 16.739 benutzt aus 16.817 ⓘ

+ Domains mit Schadsoftware (2/4)

[Malware Domain List](#) 1.105 benutzt aus 1.105 ⓘ

[Malware domains](#) 🏠 26.887 benutzt aus 26.902 ⓘ

+ Belästigungen (4/6)

[AdGuard Annoyances](#) 🏠 ⓘ 17.176 benutzt aus 19.080 ⓘ

[Fanboy's Cookie List](#) 🏠 14.543 benutzt aus 14.548 ⓘ

[Fanboy's Annoyance List](#) 🏠 12.448 benutzt aus 52.708 ⓘ

[Fanboy's Social Blocking List](#) 🏠 25.501 benutzt aus 25.509 ⓘ

+ Verschiedene Zwecke (1/4)

[Peter Lowe's Ad and tracking server list](#) 🏠 2.967 benutzt aus 2.967 ⓘ

+ Regionen, Sprachen (1/37)

[DEU: EasyList Germany](#) 🏠 9.353 benutzt aus 9.355 ⓘ

Cookie AutoDelete



- Automatisiertes Löschen von Cookies nach dem Schließen von Browser-Fenstern und -Tabs.
- Kann auch den LocalStorage leeren.

The screenshot shows the Cookie AutoDelete interface for the domain **spiegel.de**. At the top, there are four buttons: a green button for "Automatisches Aufräumen aktiviert", a red button for "Benachrichtigung deaktiviert", a yellow button for "Aufräumen" with a dropdown arrow, and a blue button for "Einstellungen". Below this, the domain **spiegel.de** is listed with a red 'S' icon. Underneath, there are two entries: "spiegel.de" and "*.spiegel.de". Each entry has two buttons: a grey button with a plus sign and the text "Greylist" and a blue button with a plus sign and the text "Whitelist". At the bottom, a light blue box contains the text "Keine Regeln passen zu dieser Domain".

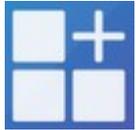
NoScript



- Zum Blockieren von Skripten/JavaScript.
- Blockiert standardmäßig zunächst alle Skripte (Black-List-Modus)
- Kann auf einen White-List-Modus umgestellt werden (nicht empfohlen).



Noch mehr Add-ons!



- **Firefox Multi-Account Containers**

- Zugriff auf Cookies isolieren.



- **Decentraleyes**

- Externe JavaScript-Bibliotheken lokal ausliefern.



- **Neat URL**

- Entfernt Tracking-Parameter aus URLs.



- **Smart Referer**

- Referrer nicht beim Wechseln der Website senden.



- **uMatrix**

- Mächtiger Inhaltsblocker / Website-Firewall. **Vorsicht!**

Kontrolle

- Wirkung von Add-ons und Einstellungen kontrollieren:
 - Add-On: **Lightbeam**
 - Menü → Extras → Webentwickler → Netzwerk

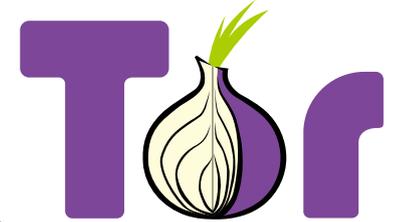
Weitere Firefox-Funktionen

- **Privater Modus**
- Keine Speicherung von Daten besuchter Webseiten **auf dem eigenen** Computer (insb. keine Chronik, keine URL-Vervollständigung, Cookies, etc.)
- Auf dem lokalen System verbleiben keine Spuren
- *Keine Anonymität* gegenüber dem Netz



Sie surfen im privaten Modus

Anonym surfen mit dem Tor-Browser



- Tor: **T**he **O**nion **R**outer
 - Netzwerk zur Anonymisierung von Verbindungsdaten
 - IP-Adresse wird verschleiert
 - Effektive Maßnahmen gegen Tracking schon implementiert

Vorteile

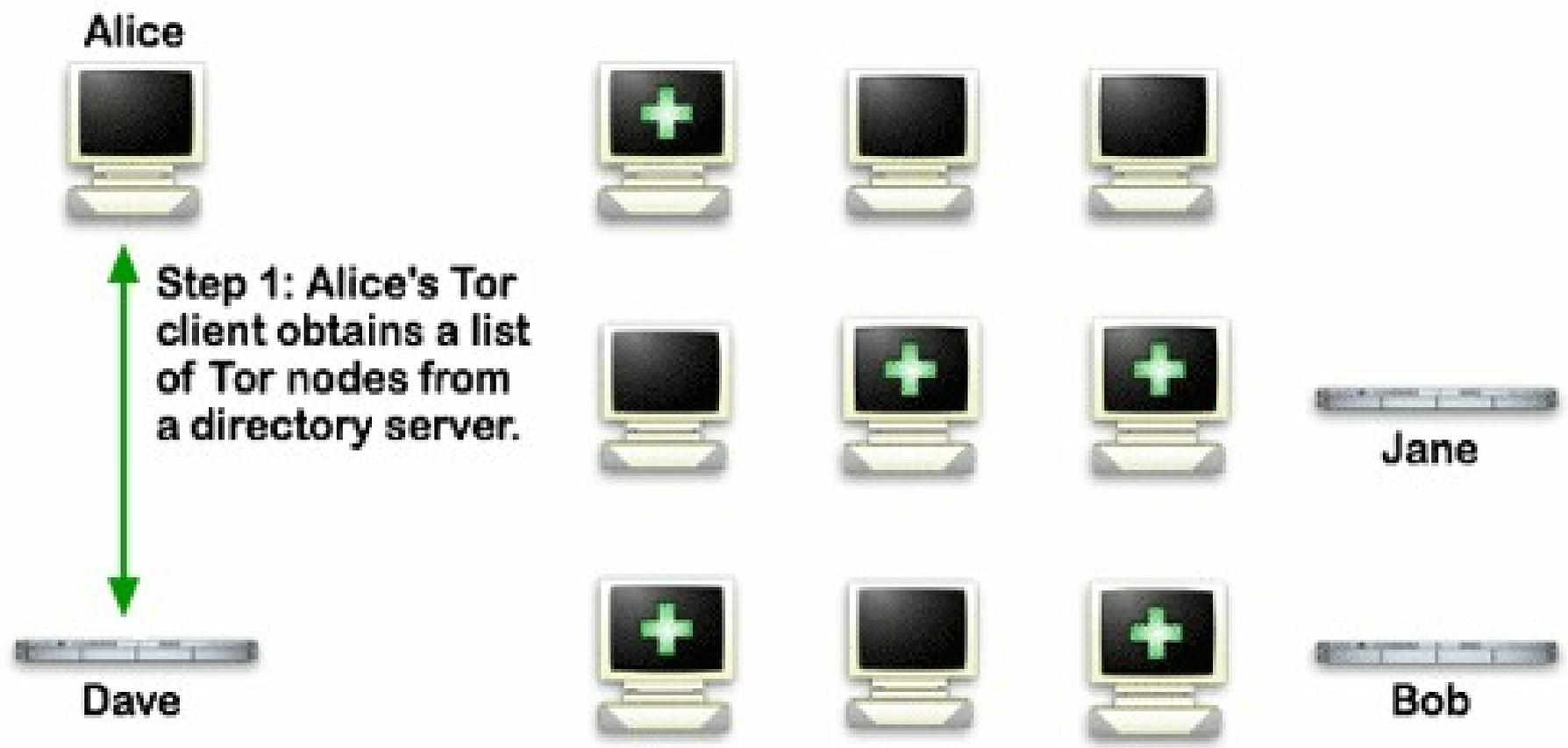
- Quelloffen, freie Software
- Anonymes Surfen

Nachteile

- Login bei personalisierten Seiten nicht sinnvoll
- Latenz ist größer

How Tor Works: 1

-  Tor node
-  unencrypted link
-  encrypted link



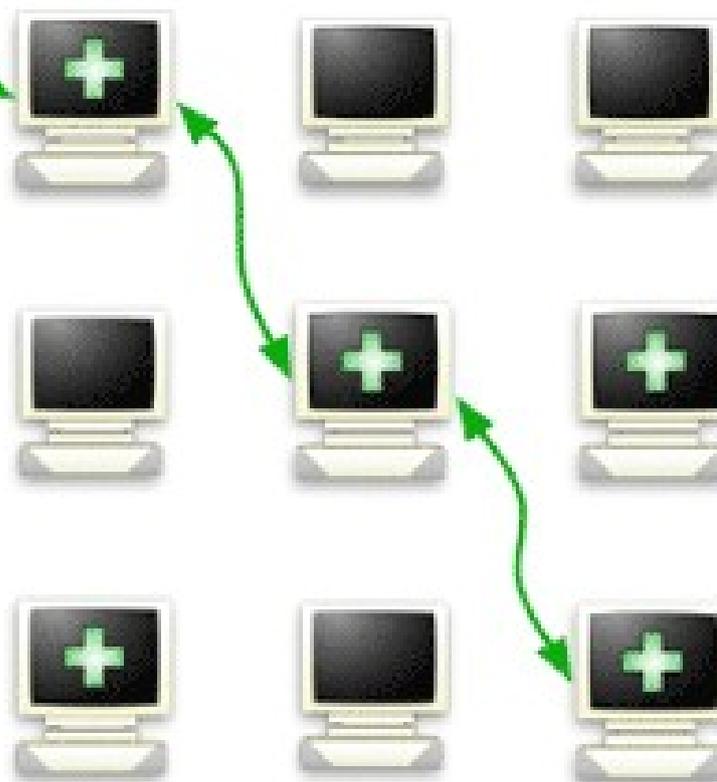
How Tor Works: 2



Alice



Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.



Dave



Jane

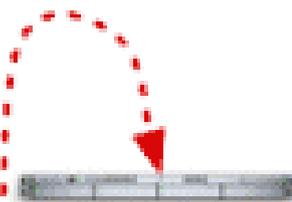


Bob

E How Tor Works: 3

-  Tor node
-  unencrypted link
-  encrypted link

Alice



Jane



Bob

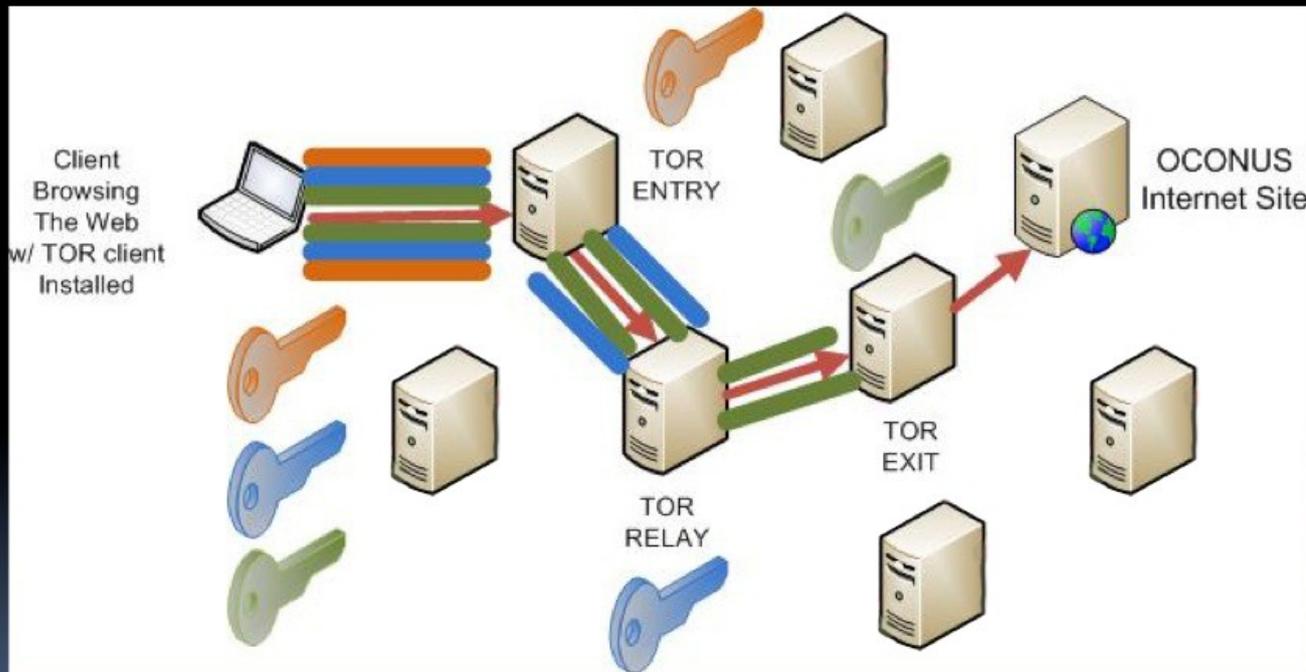
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, **green links** are encrypted, **red links** are in the clear.



Dave



(U) What is TOR?



Download Tor-Browser

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

Über Tor - Tor-Browser

Über Tor x +

Tor-Browser Suche oder Adresse eingeben

Nutzen Sie Tor-Browser das erste Mal? Schauen Sie sich diese kleine Einführung an.

Tor-Browser 8.0.9

Entdecken. Privat.

Du bist bereit für das privateste Browsing-Erlebnis der Welt.

Tor-Browser-Sicherheitseinstellungen

Sicherheitsstufe

Am sichersten Erlaubt nur Webseiten-Funktionen, die für statische Seiten und Basisdienste benötigt werden. Diese Änderungen betreffen Bilder, Medien und Skripte.

In der sichersten Einstellung:
JavaScript ist standardmäßig auf allen Seiten deaktiviert.

Sicherer Einige Schriftarten, Symbole, mathematische Symbole und Bilder sind deaktiviert.
Audio und Video (HTML5-Medien) müssen zur Wiedergabe angeklickt werden.

[Erfahre mehr](#)

Standard

Abbrechen OK

Tails – ein OS für Tor

- The **A**mnestic **I**ncognito **L**ive **S**ystem (Tails)
- Live-Linux-DVD / USB
- Anonymität als erstes Designprinzip
- Viele Tools
 - Pidgin
 - Electrum
 - MAT
 - KeePassX



Exkurs: Apps auf dem Smartphone

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 (netzwerkbasierend)
 - Genauer Standort (GPS- und netzwerkbasierend)
- 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

10

trackers

26

permissions



Lieferando.de - Order Food

Version: 6.1.4

Creator: Takeaway.com

Downloads: 5,000,000+ downloads

Other versions

On Google Play

APK fingerprint

This report was automatically issued on May 8, 2019, 6:12 a.m..

This report was automatically updated on May 8, 2019, 6:12 a.m..



Finger
Issuer:
Subjec
Serial:

10 Trackers

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

- Ad4Screen
- Adjust
- Facebook Analytics
- Facebook Login
- Facebook Places
- Facebook Share
- Google Analytics
- Google CrashLytics
- Google Firebase Analytics
- HockeyApp

26 Permissions

We have found the following permissions in the application: (2 **Special** 2 **Dangerous**)

- ACCESS_COARSE_LOCATION (android.permission)
Access Approximate Location (Network-based)
- ACCESS_FINE_LOCATION (android.permission)
Access Precise Location (GPS And Network-based)
- ACCESS_NETWORK_STATE (android.permission)
View Network Connections
- ACCESS_WIFI_STATE (android.permission)
View Wi-Fi Connections
- INTERNET (android.permission)
Have Full Network Access

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.
- Falls verfügbar: Datenschutzmodus aktivieren!
- Alternative Apps nutzen, die weniger Berechtigungen benötigen.

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

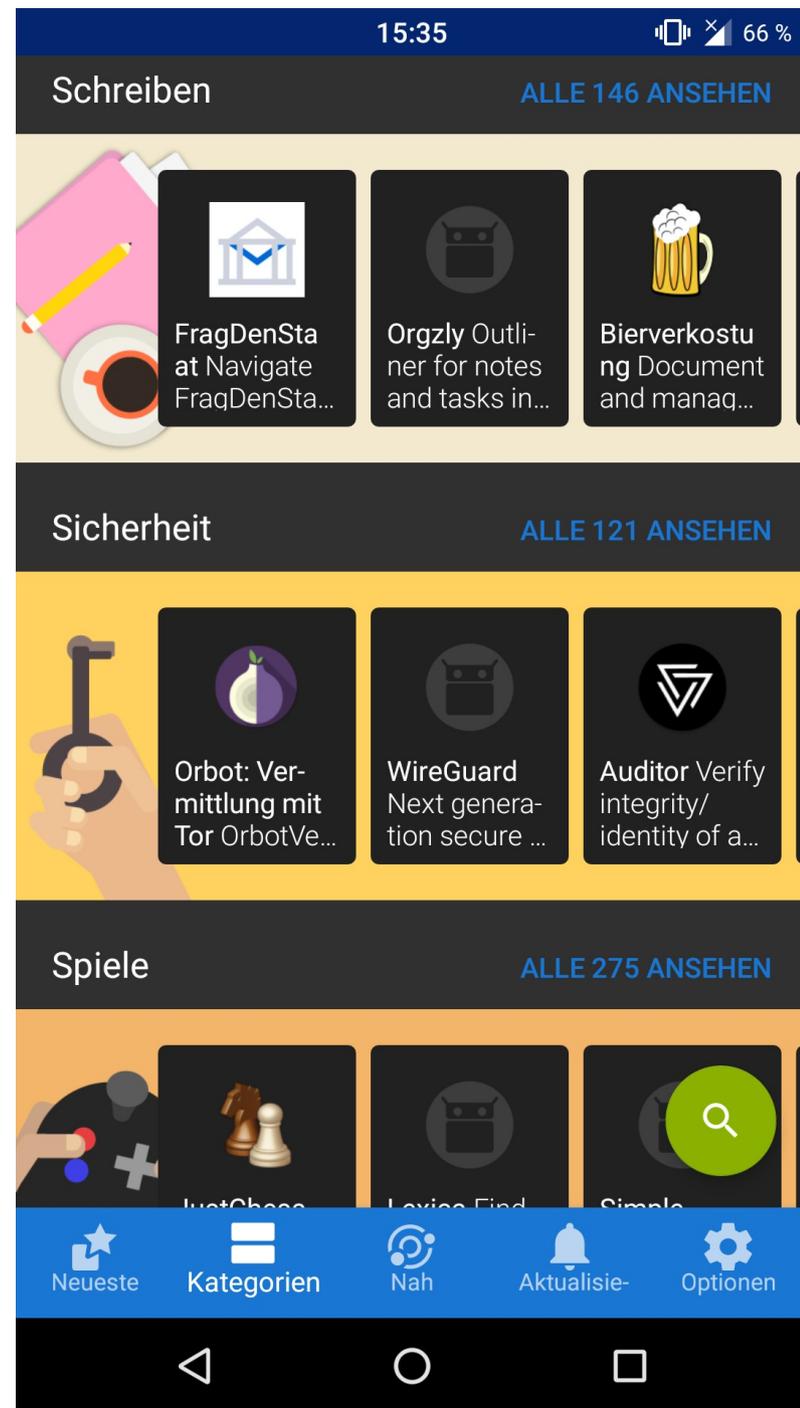
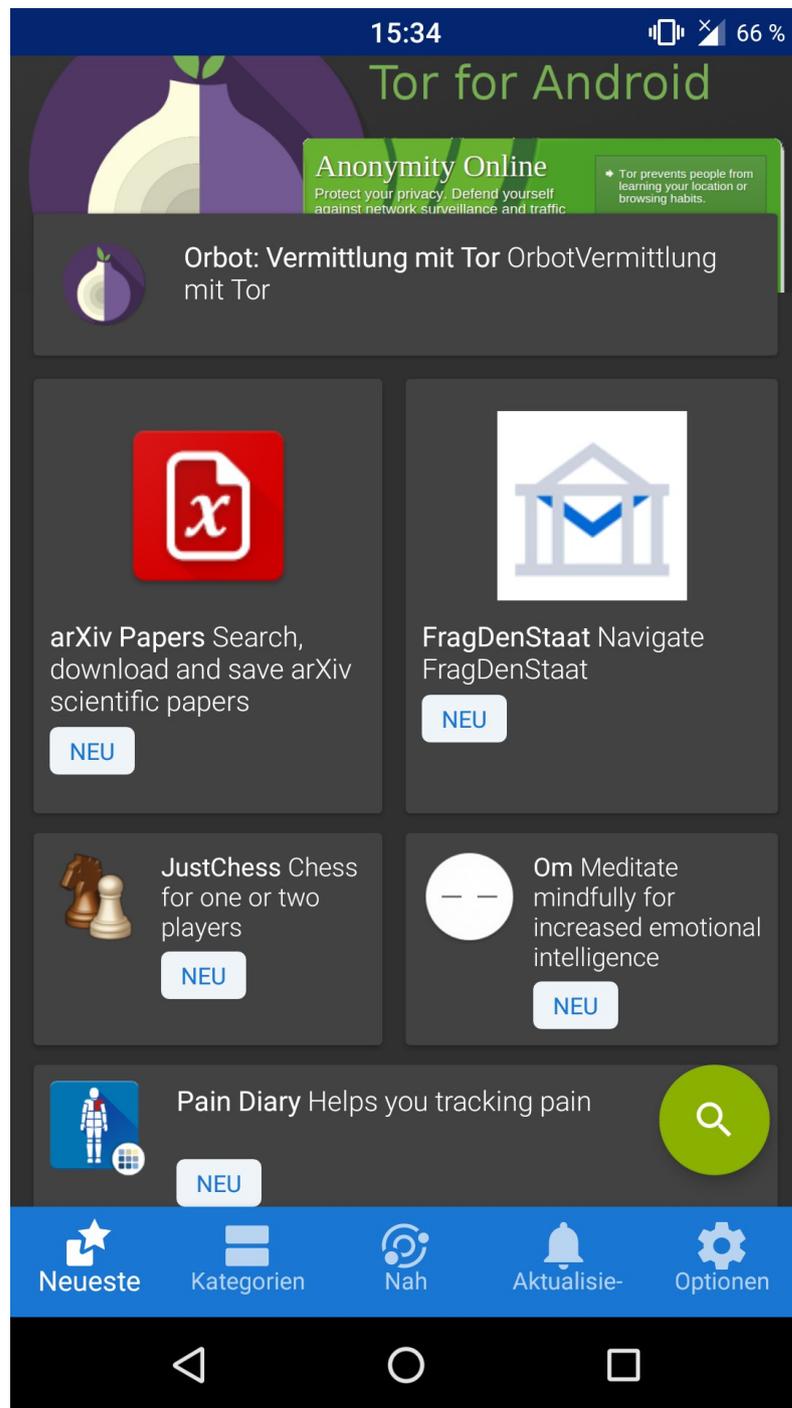
4. Freie Android-Variante installieren

- 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)





Leseempfehlungen

- **Mike Kuketz: Firefox-Kompendium**
 - <https://www.kuketz-blog.de/firefox-ein-browser-fuer-datenschutzbe-wusste-firefox-kompendium-teil1/>
- **Privacy-Handbuch: Spurenarm Surfen**
 - https://www.privacy-handbuch.de/handbuch_21.htm
- **Broschüren, Flyer und Handouts zum Mitnehmen!**

Digitalcourage in der Nähe

- **Ortsgruppe Bremen**

- <https://digitalcourage.de/treffen-vor-ort/bremen>
- Treffen an jedem zweiten Dienstag im Monat um 18:00 Uhr im „Ausspann“ (Schnoor 1–2 im Bremer Schnoor-Viertel).

- **Ortsgruppe Braunschweig**

- Die Ortsgruppe trifft sich jeden zweiten Donnerstag um 18:30 Uhr im „Stratum 0“ (Hamburger Str. 273A, Eingang A2).
- <https://digitalcourage.de/treffen-vor-ort/braunschweig>

Weitere Veranstaltungen

- Praxis der digitalen Selbstverteidigung
 - Samstag, 11. Mai 11 - 16 Uhr Raum A01 0-010b
- Digitalisierung und Gender (revisited)
 - Mittwoch, 15. Mai 18 Uhr A10 Hörsaal F
- Diskriminierung durch Software
 - Samstag, 18. Mai 11 - 16 Uhr Raum A01 0-010a
 - Achtung: Dieser Workshop ist nur für FrauenLesbenInterNonbinaryTrans* Personen.
- <https://uol.de/hib/veranstaltungen/>

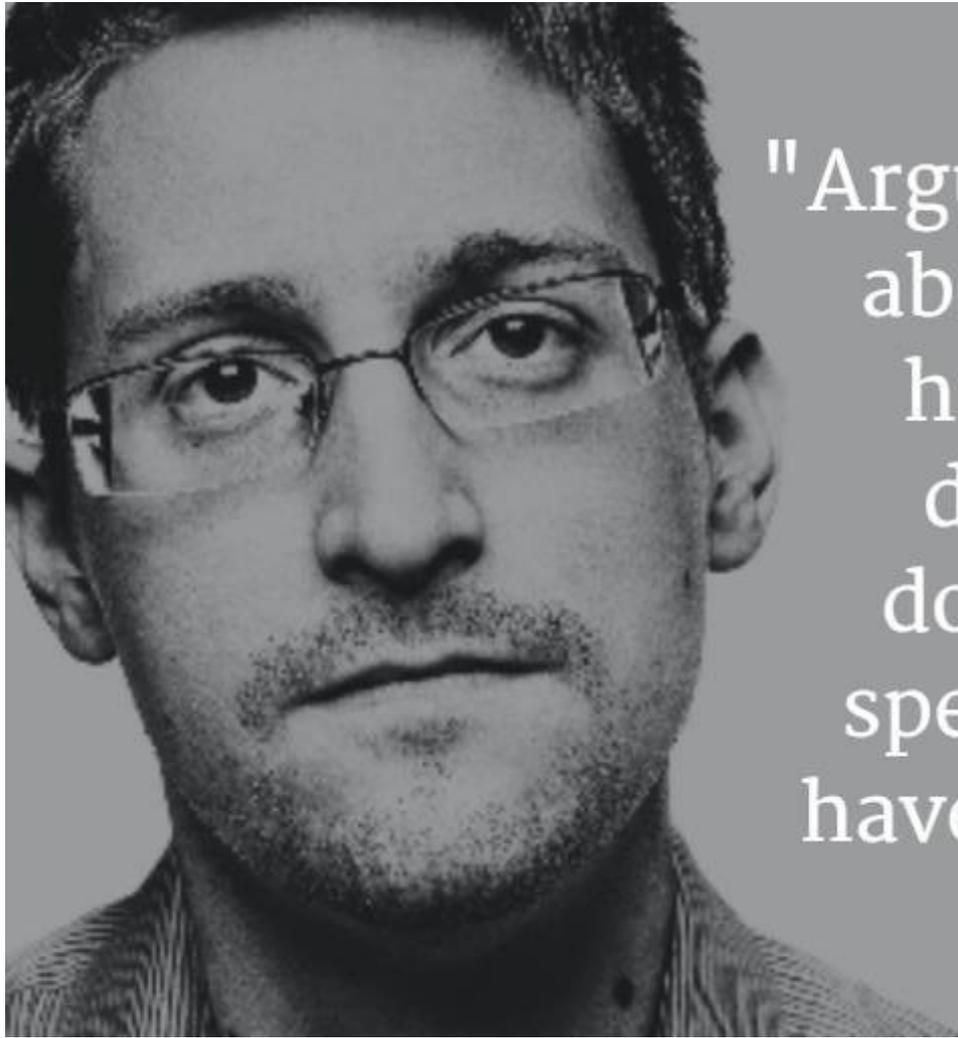
Kryptocafé in Oldenburg

- Themen:
 - Browser (Praxis!)
 - Verschlüsselte Mails & Messenger
- Wann?
 - Freitag, 10. Mai, 18-20 Uhr
- Wo?
 - VBZ Oldenburg, Justus-Moser-Platz 5

Ich habe nichts zu verbergen – oder doch?

Nichts zu verbergen? Blödes Argument!

- Geheimnisse sind sozial etwas Essenzielles.
- Wir wissen nicht, wie Daten über uns in Zukunft verwendet werden.
- Nicht alles was verbergen wird, ist illegal.
- Es ist unsolidarisch.
- Es verhindert Widerstand.



"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."