



Cryptoseminar Bielefeld

Digitale Selbstverteidigung gegen Massenüberwachung

Kurze Vorstellung

- Georg Gottleuber
- Sebastian Liskén
- Leif Rottmann
- Jan Schötteldreier
- Julia Barthel

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
 - Crypto-Partys
 - Backup-Partys
 - Linux-Install-Partys
 - 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>





**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

Agenda

von	bis	Titel
09:00	10:00	Vortrag: Motivation – Eine Einführung in den Datenschutz?
10:00	10:30	Social Media
10:30	10:40	- Kurze Pause -
10:40	11:40	Browser
11:40	12:10	Praxis
13:00	14:00	- Mittagspause -
14:00	14:30	E-Mail
14:30	14:40	- Kurze Pause -
14:40	15:10	Mobilgeräte
15:10	17:00	Praxis, Open End

<https://digitalcourage.de/hsg>

Privatsphäre im Zeitalter der Massenüberwachung – Eine Einführung in den Datenschutz

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 „empfänglich“ [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

Verletzung der Privatsphäre

- Erpressbarkeit
- Chilling Effects
- ...

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 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/>



**Ich weiß, was du letzten
Sommer gesucht hast!**

Google

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..



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

Constanze Kurz, Chaos Computer Club

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)

Facebook

- „Kostenlos“
- Datenschutzeinstellungen werden immer schwieriger
- Klarnamenpflicht
- Rechte an den Daten
- Intransparenz bei der Weitergabe
- Lock-In (kein Profil-Export)

Schön zusammengefasst von Alexander Lehmann (für X3)

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

Datenwirtschaft

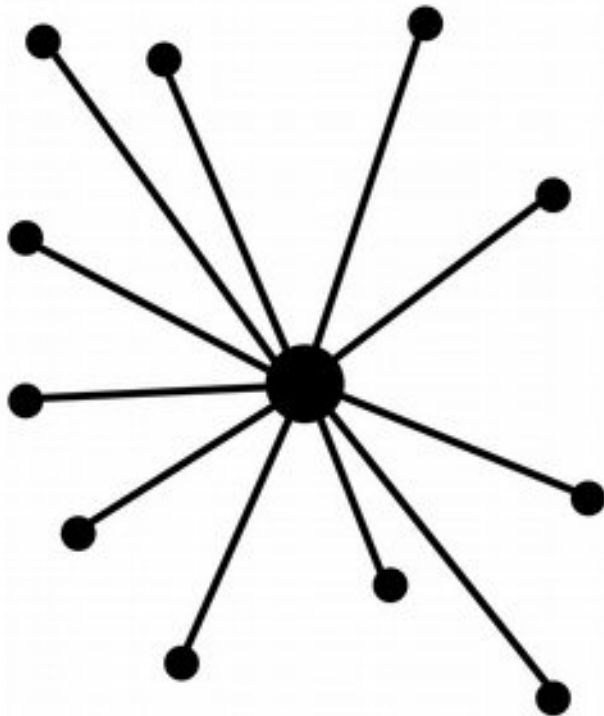
- "Kostenlose" Angebote
 - Daten sind eine neue Währung
 - Datenhändler kaufen Profile und verkaufen sie an die Werbeindustrie, Versicherungen, Schufa, etc.
- Geschlossene Systeme
 - Proprietäre Software
 - Keine offenen Schnittstellen
- Big Data
 - Zusammenführung, Analyse und Auswertung großer Datenmengen

Datenwirtschaft

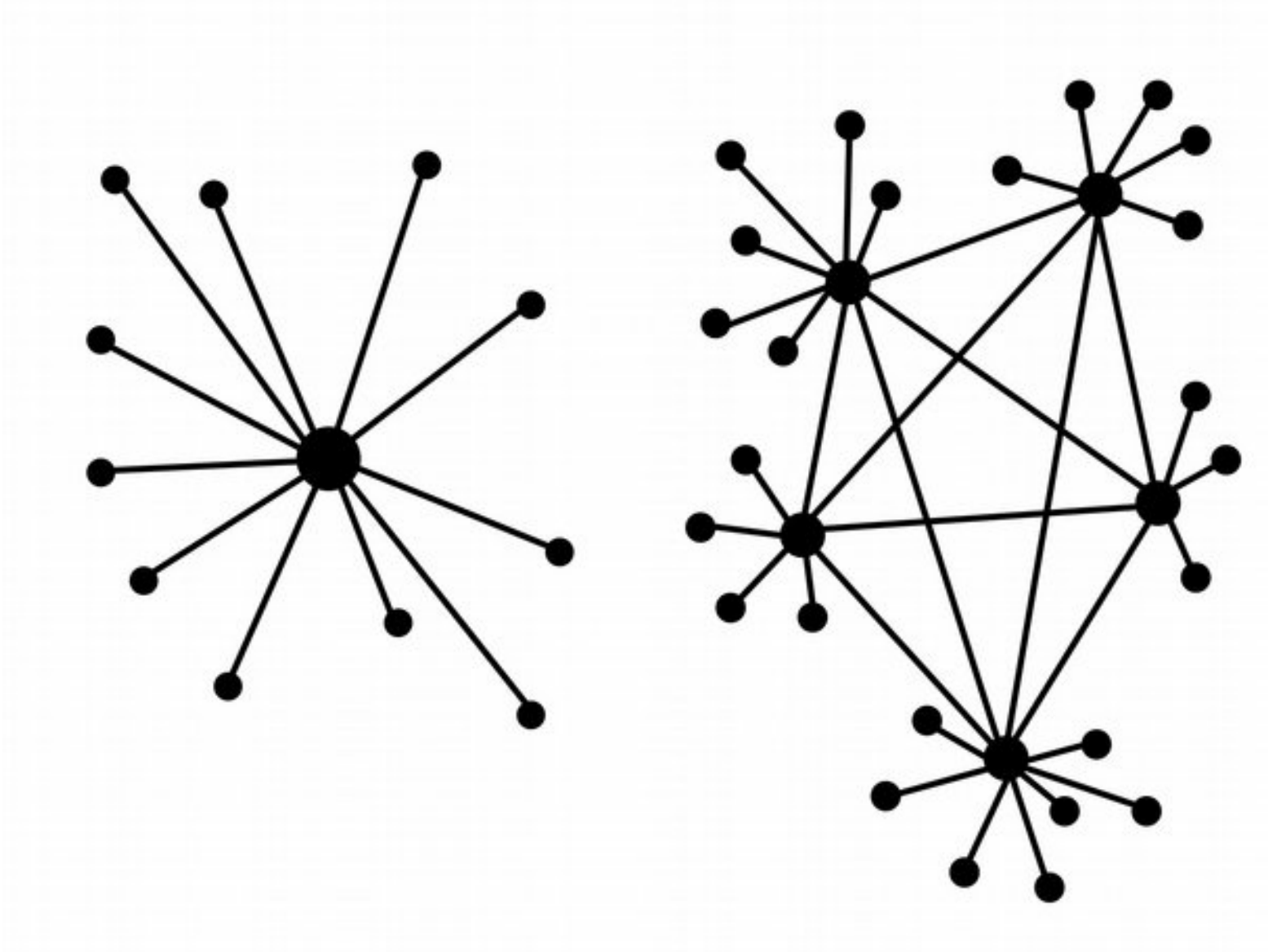
- Sicherheit
 - Bedeutet Aufwand = Kosten
- Datenschutz
 - Weniger Daten für das Unternehmen
 - Weniger Rohmaterial zum Analysieren und Verkaufen
 - Privatsphäre "überholt"?

Die DSGVO hat Datenschutz in Europa wieder stark gemacht

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 „Twelve 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

VDS (Historie)

- 2006: EU-Richtlinie
 - Nach und nach von vielen Mitgliedsstaaten umgesetzt
- 2010: Vom Bundesverfassungsgericht als verfassungswidrig erklärt
- 2014: Vom EuGh wegen Verstoß gegen die Charta der Grundrechte als ungültig erklärt

VDS-Zombie

- 2015 vom Bundestag beschlossen als:

„Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten“.

- Anfang 2017: Bundesverfassungsgericht lehnt Klärung im Eilrechtsschutzverfahren und Aufschub ab.
- Ab 1. Juli startet Speicherpflicht
- Verfassungsbeschwerden laufen

Neusprech Award 2015

- Vorratsdatenspeicherung
- Mindestspeicherfrist, Mindestspeicherdauer
- Mindestdatenspeicherung
- Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten
- Private Vorsorgespeicherung
- Digitale Spurensicherung

VDS: Wer speichert?

- Telekommunikationsanbieter
 - ISP (Internet-Service-Provider) & Mobilfunkanbieter
 - Outsourcing: VDS as a Service
- Polizeibehörden fordern Daten zur Aufklärung "schwerer Straftaten" an.

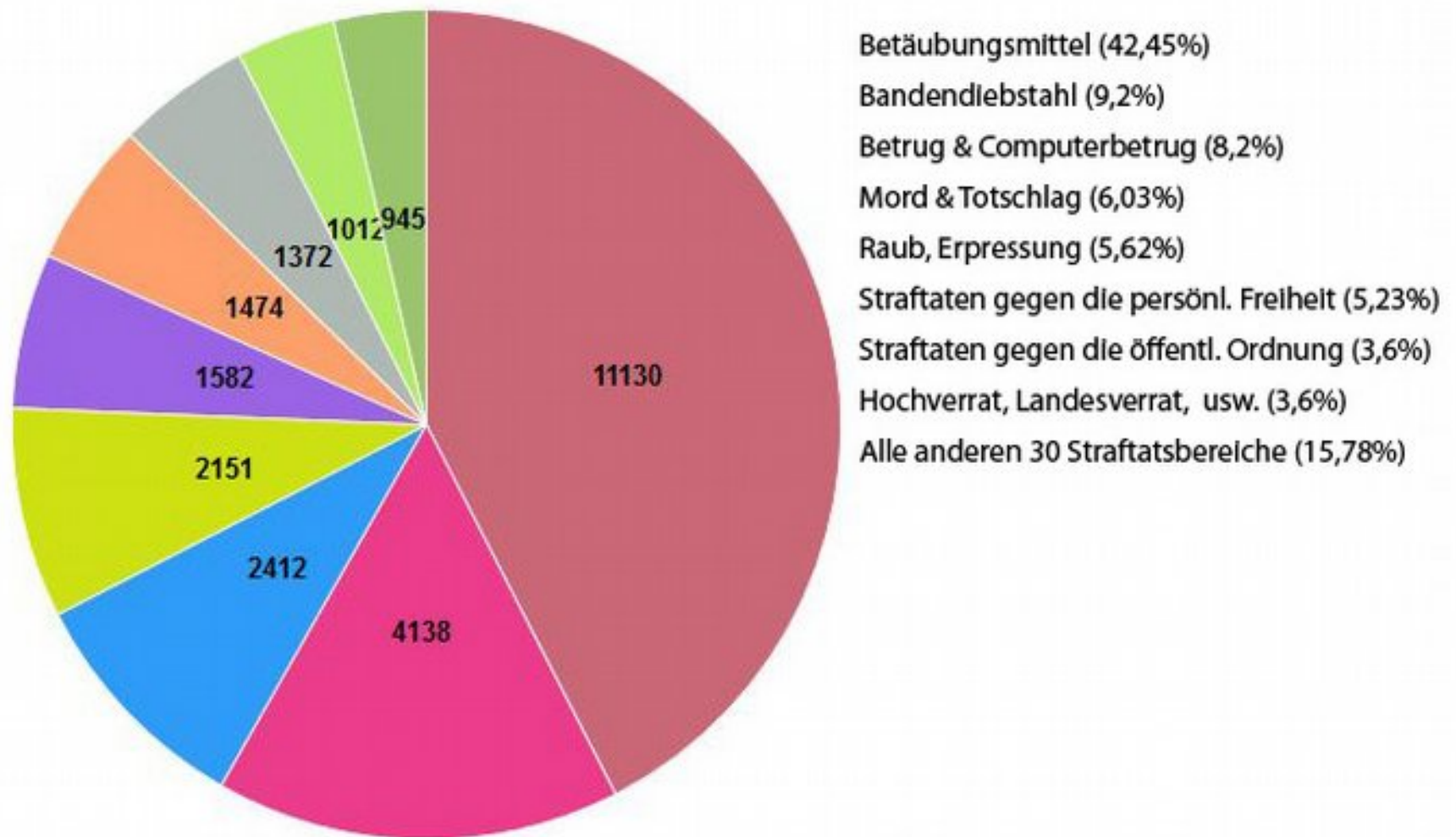
VDS: Was wird gespeichert?

- Standortdaten **aller Mobiltelefonate** bei Beginn des Telefonats (für 4 Wochen)
- Standortdaten bei Beginn einer **mobilen Internetnutzung** (für 4 Wochen)
- Rufnummern, Zeit und Dauer **aller Telefonate** (für 10 Wochen)
- Rufnummern, Sende- und Empfangszeit **aller SMS-Nachrichten** (für 10 Wochen)
- Zugewiesene IP-Adressen **aller Internetnutzer** sowie Zeit und Dauer der Internetnutzung (für 10 Wochen)

VDS Visualisierung

- Balthasar Glättli (Grüne, Schweiz):
<https://www.digitale-gesellschaft.ch/vorratsdatenspeicherung/>
- Malte Spitz (Grüne, Deutschland):
<http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten>

TELEKOMMUNIKATIONSÜBERWACHUNG 2015 NACH STRAFTATBESTÄNDEN



Quelle: Netzpolitik.org

VDS: Ausweitung

- Schon vor in Kraft treten des Gesetzes
- Vorratsdaten auch bei Wohnungseinbrüchen abfragen
 - Zusätzlich Funkzellenabfrage
- Kritik: Technik erst etablieren, dann ausweiten

Folgen von Massenüberwachung

- Alle Bürger sind Verdächtige
- Schere im Kopf
 - Selbstzensur
- Chilling Effect
 - Angepasstes Verhalten
- Einschränkung vieler Grundrechte
 - Meinungsfreiheit, Briefgeheimnis, Freie Entfaltung der Persönlichkeit

Massenüberwachung durch die NSA

- Stasi vs. NSA Flächenvergleich:
<https://apps.opendatacity.de/stasi-vs-nsa/>

Leseempfehlungen

- <https://netzpolitik.org>
- Buch: "Die globale Überwachung" (Glenn Greenwald)
- Buch: "Was Google wirklich will" (Thomas Schulz)
- Videos: <http://www.alexanderlehmann.net/>

Social Media



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.

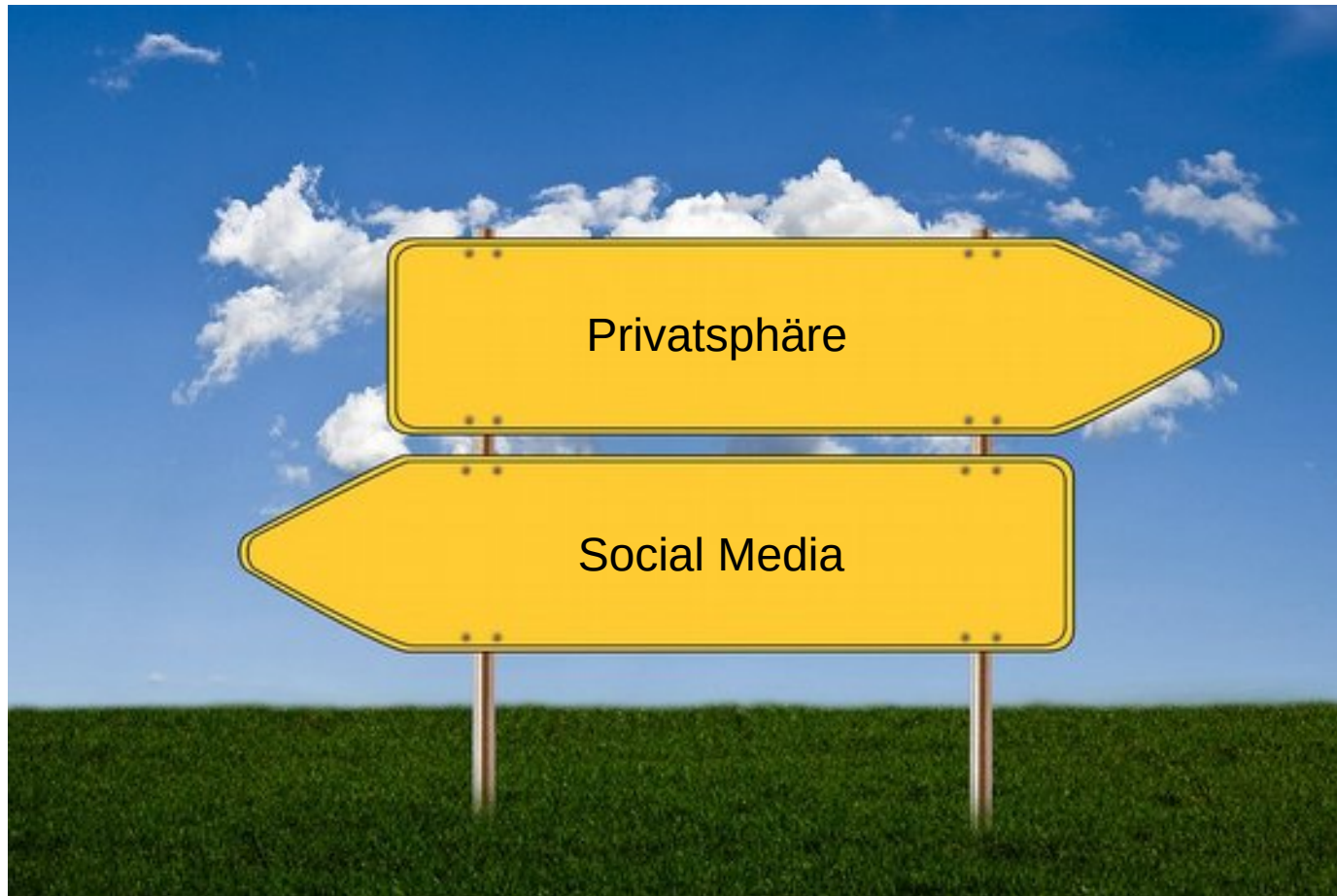


Pflicht zur Benutzung von Social Media im Arbeitsleben?

- Direktionsrecht des Arbeitgebers
- Technische Ausgestaltung des Produkts und organisatorische Maßnahmen des Arbeitgebers
- Notwendig für Geschäftsbetrieb?
 - Kundenkontakt oder PR-Abteilung



Umgang mit Social Media



Rechte Dritter beachten

Recht am eigenen Bild

Personenbezogene Daten; auch
Telefonnummer

Konsequenzen bei Äußerungen
beachten



Handlungsempfehlungen

- Sorgfältiger Anmeldeprozess
- "Richtige Netzwerk" auswählen und
- Wirkungsgrad vorab festlegen
 - Private oder geschäftliche Nutzung?
 - Welche Inhalte und wozu gedacht etc.
- Separate E-Mail-Adresse für Soziale Netzwerke
- Nach Möglichkeit Pseudonym verwenden
- Nicht jedes Profil wahllos als Freund hinzufügen

Handlungsempfehlungen

- Profil für Suchmaschinen unsichtbar machen
- Sichtbarkeit von Kontaktdaten auf "für niemanden sichtbar" stellen
- Oder zumindest Sichtbarkeit von Inhalten überdenken
 - Beiträge, Profilbilder, Fotoalben...
 - Prämisse: Je weniger, desto besser
- Kontaktsuche durch hochladen des Adressbuchs verhindern
 - ZB bei LinkedIn, Xing, etc.

Handlungsempfehlungen

- Kein Hochladen von Fotos auf denen anderen Personen zu sehen sind und diese nicht markieren
- Dritte vorher um Erlaubnis fragen!
- Bitte Foto zu löschen schnellstmöglich nachkommen
- Alternative Kommunikationsplattformen nutzen
- Aus Facebook/Twitter etc. raus linken, nicht hinein
- Ablehnung und Alternativen kundtun

Was spricht gegen Facebook?

- Mit Facebook bleibt nichts privat
- Automatische Gesichtserkennung möglich (in Europa deaktivierbar)
- Mit Facebook fühlt man sich schlechter
- Ständige personalisierte Werbung
- Facebook verdient Geld mit Desinformation

Was spricht gegen Facebook?

- Hass und Hatespeech
- Steuervermeidung in großem Stil
- Konsumenten- und Wählermanipulation durch Datenanalyse
- Unbemerkte individuelle Manipulation einer Vielzahl von Menschen

Was spricht gegen Facebook?

- Zeitverschwendung durch Katzenvideos
- Immer wieder Verstöße gegen europäisches Datenschutzrecht
- Profile von Nicht-Usern, zB durch Tracking über Websites (Like-Button)
- FB entscheidet über unser Leben
 - Patent zum Kreditscoring

Fediverse

- Federated Universe
- Dezentrales Kommunikationsnetz
- Freie Server-/Anbieter auswahl (sog. Instanzen)
- Derzeit c.a. 1,4 Millionen Nutzer – wachsend
- Nutzer einer Instanz können denen anderer Instanzen folgen

Bekannte Alternativen

- Mastodon anstatt Twitter (Instanzen unter: <https://instances.social/>)
- Friendica als Soziales Netzwerk anstelle von Facebook
- PeerTube zum hosting von Videos anstatt Youtube
- Weitere Dienste findet man zB unter <https://fediverse.party/>

Webseiten und Social Media

- Für Webseitenbetreiber – Shariff nutzen
- Open-Source-Programm verhindert sofortiges Tracking



Bildausschnitt von: <https://heiseonline.github.io/shariff/>

Shariff findet ihr hier:

<https://www.heise.de/ct/artikel/Shariff-Social-Media-Buttons-mit-Datenschutz-2467514.html>



- Kurze Pause -

Sichere Passwörter

Sichere Passwörter (2)

Wie erschwert man das Knacken des Passworts?

- Brute Force
 - Länge: 10+ Zeichen
 - Verschiedene Zeichentypen (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen)
- Listen / Wörterbuch-Angriffe
 - Kein einzelnes Wort als Passwort verwenden
 - Keine Wörter aus dem persönlichen Umfeld verwenden (Namen, Geburtsdaten etc.)
- Social Engineering
 - Niemandem(!) das Passwort verraten

Sichere Passwörter finden

- Wichtig:
 - Für jeden Dienst ein anderes Passwort verwenden!
 - (Passwörter in regelmäßigen Abständen austauschen/ändern)
- DBiR&dSd90M!
 - Merksatz: »**Der Ball ist Rund & das Spiel dauert 90 Minuten!**«
- HausLocherTasteMeloneBagger
 - Wortreihung
- 2UrN47oCfK6jAZ8xuKHioP4upPsl73
 - Passwortgenerator

Passwortverwaltung

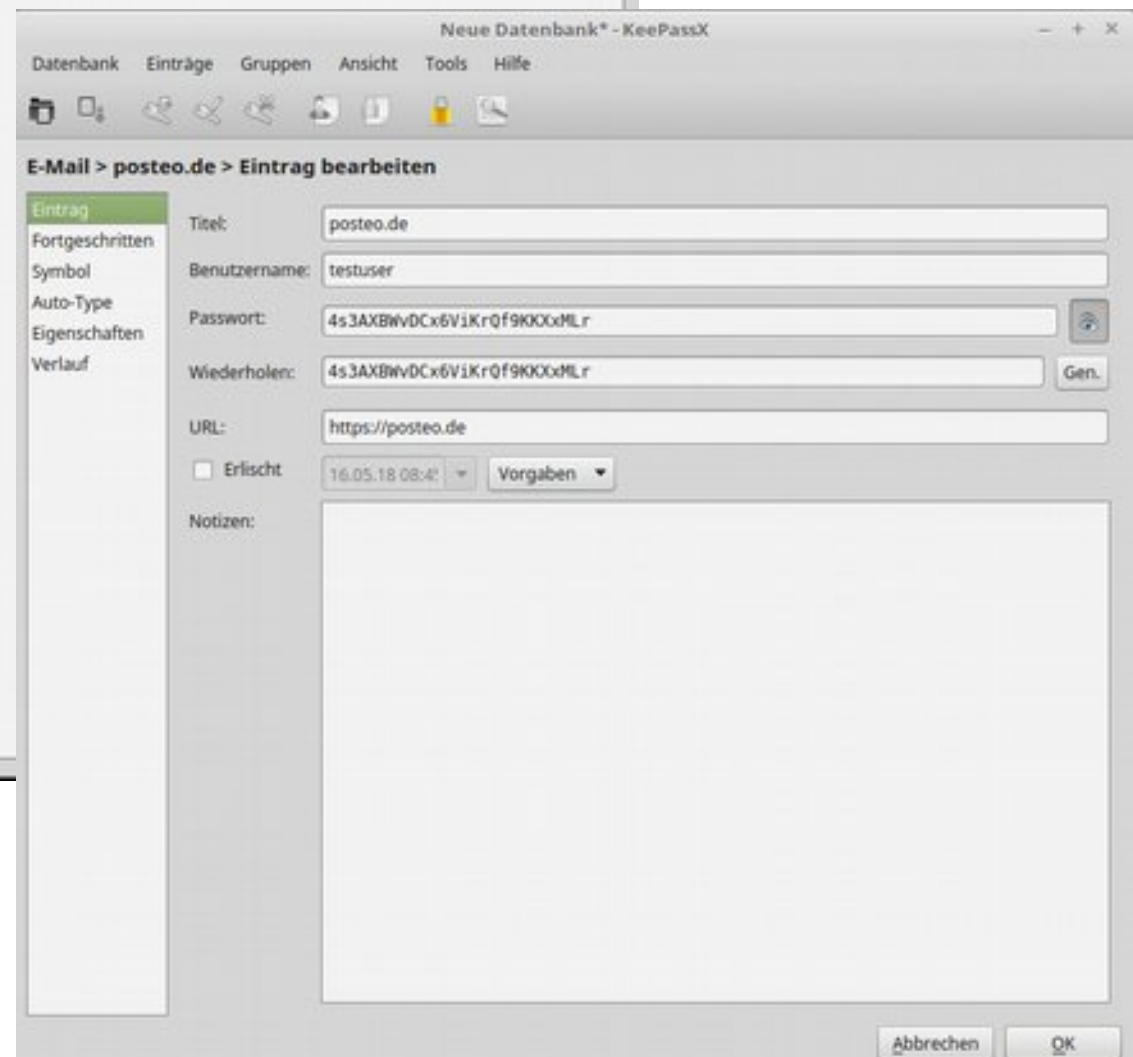
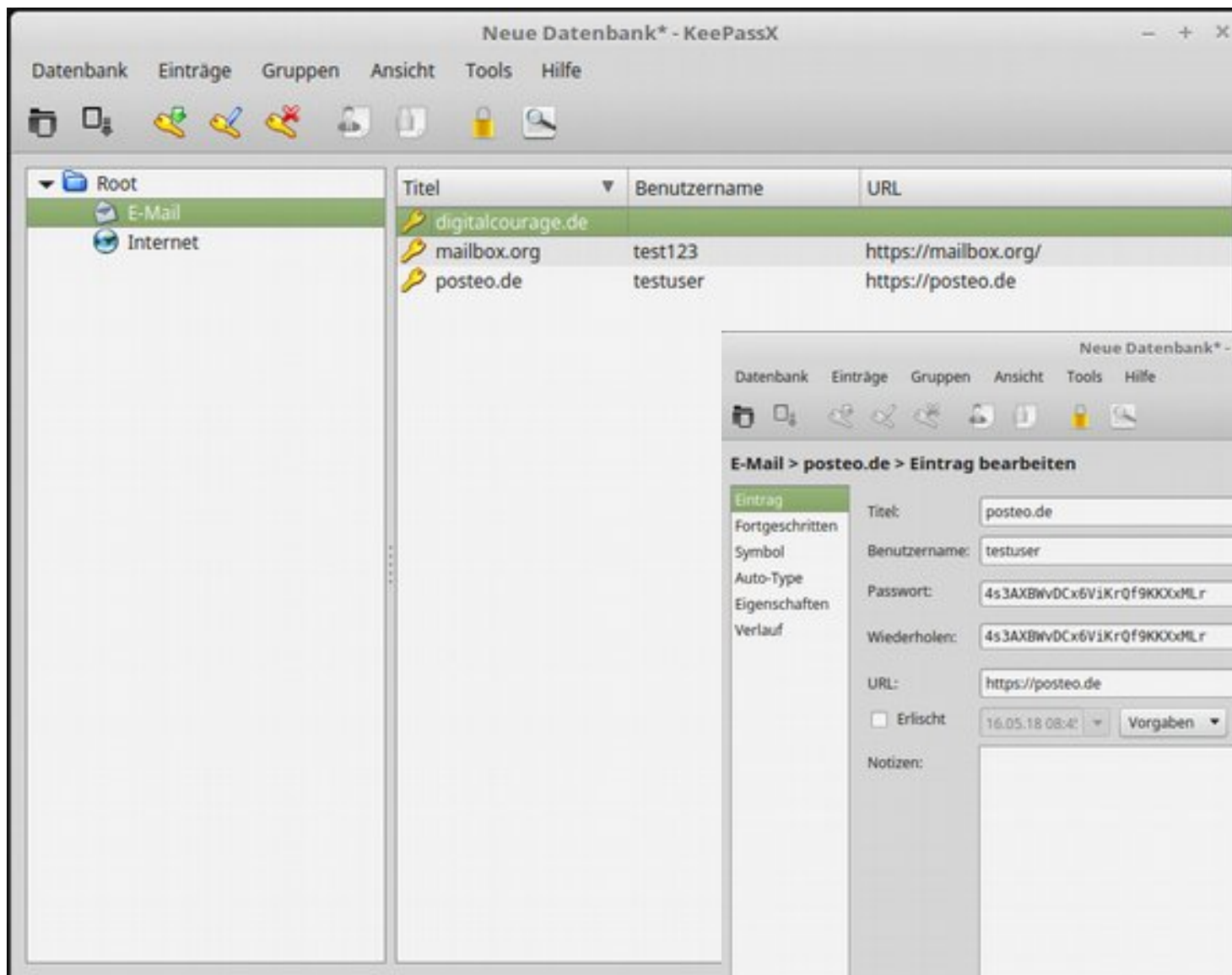
Software: **KeePassX**

Vorteile

- Freie Software
- Viele Plattformen
 - Win, Linux, Mac, Android
- Passwortgenerator
- Verschlüsselt gespeichert

Nachteile

- Masterpasswort
 - Darf nicht vergessen oder geknackt werden!
- Gefahr bei Verlust
 - „Setzt alles auf eine Karte“: PW-Datenbank gut sichern!
- Komfort
 - Kein Sync zwischen verschiedenen Geräten



Videoempfehlung

- Um das eben erklärte zu wiederholen, seht Euch bitte das Video von Alexander Lehmann " Passwörter Einfach Erklärt" an; abrufbar unter: <https://vimeo.com/138839266>

Sicher unterwegs im Internet: Browser mit Privatsphäre



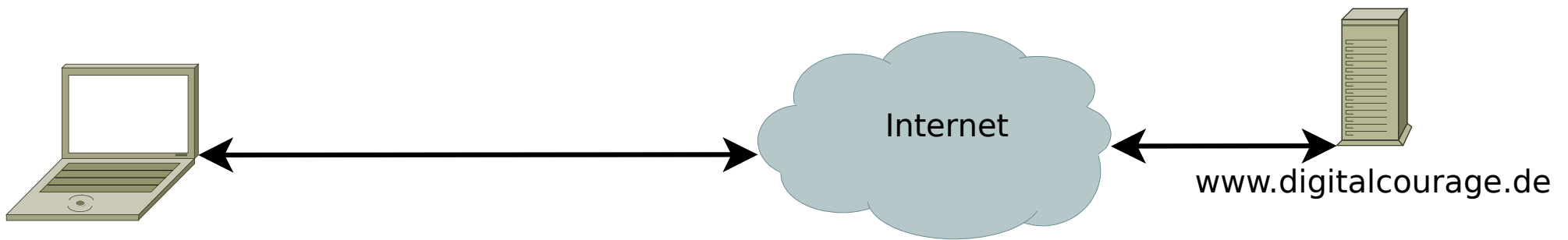
Julia



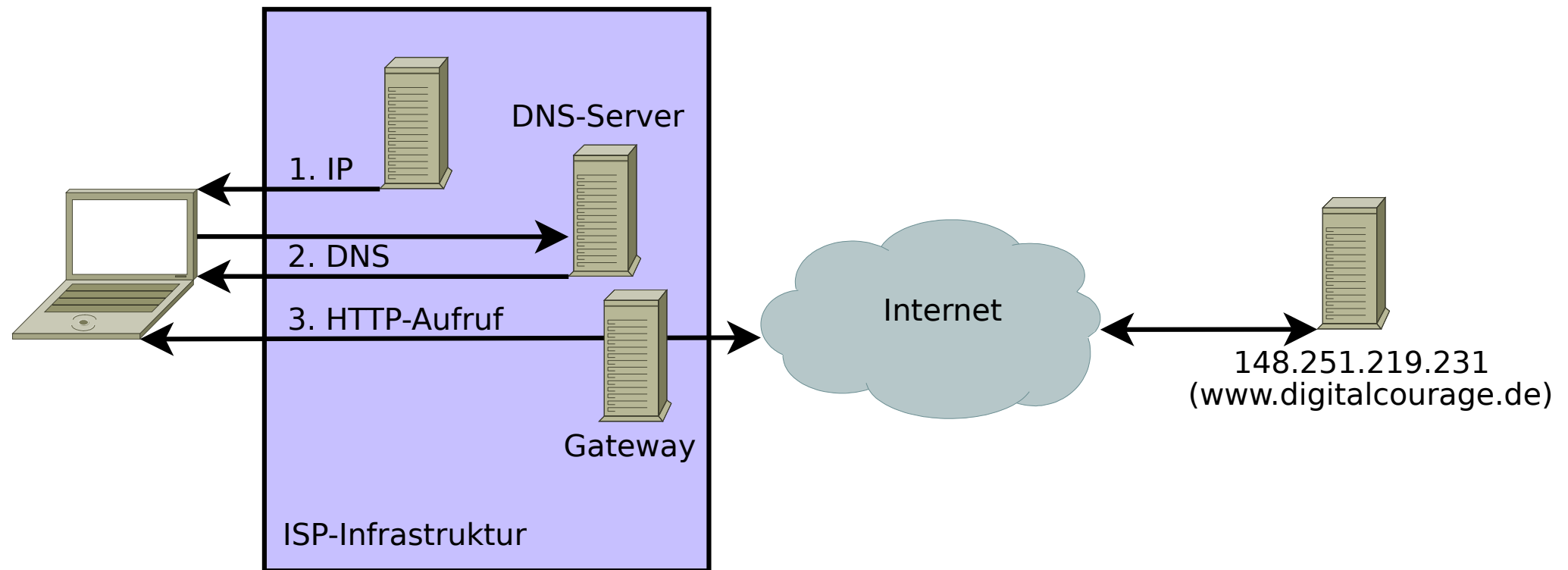
Digitalcourage e.V.

- 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*](http://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

Wie funktioniert das Internet?



Und technisch?



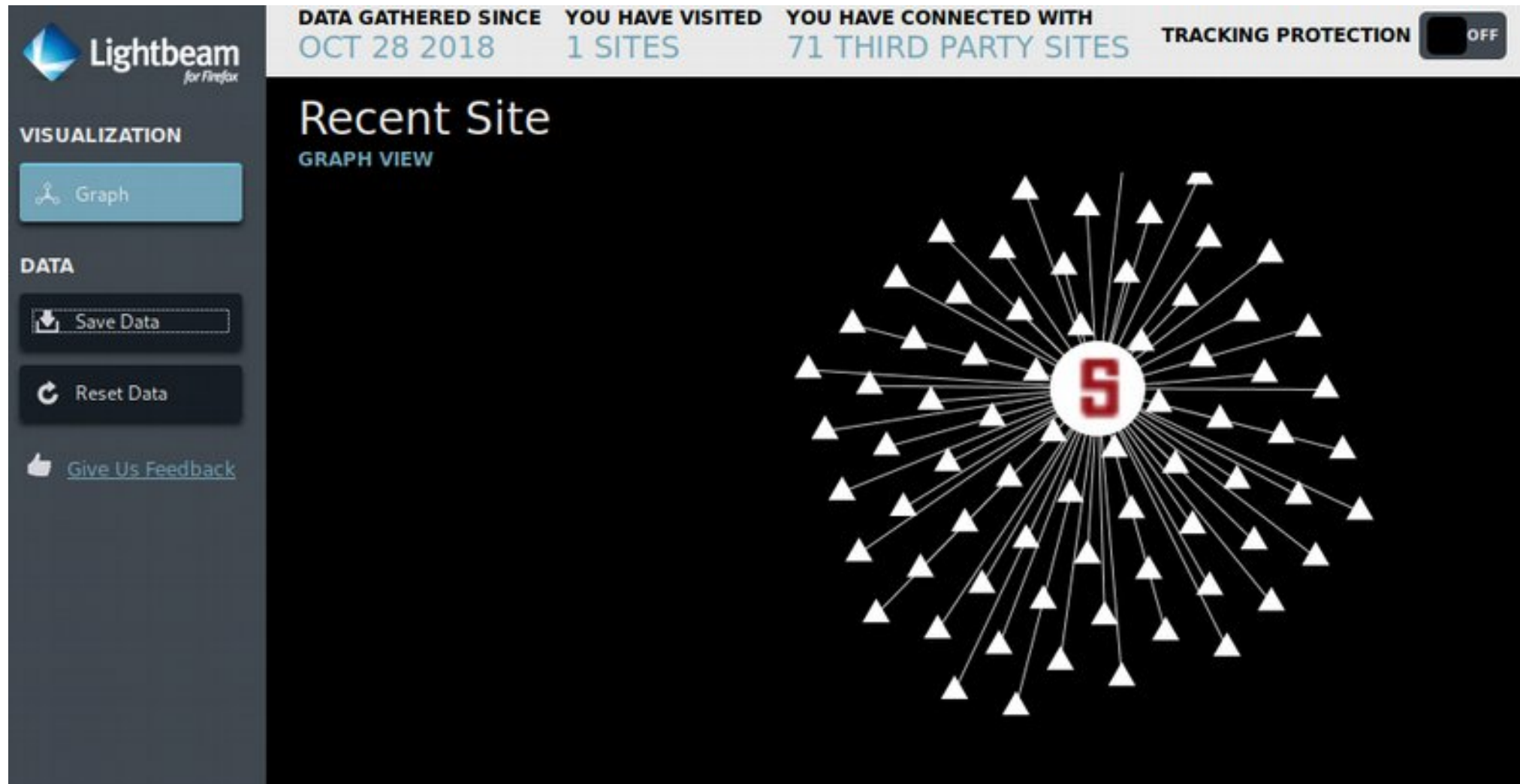
Wie schrecklich ist die Web-Realität?

- 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

Analyse in Firefox mit Lightbeam



VISUALIZATION

Graph

DATA

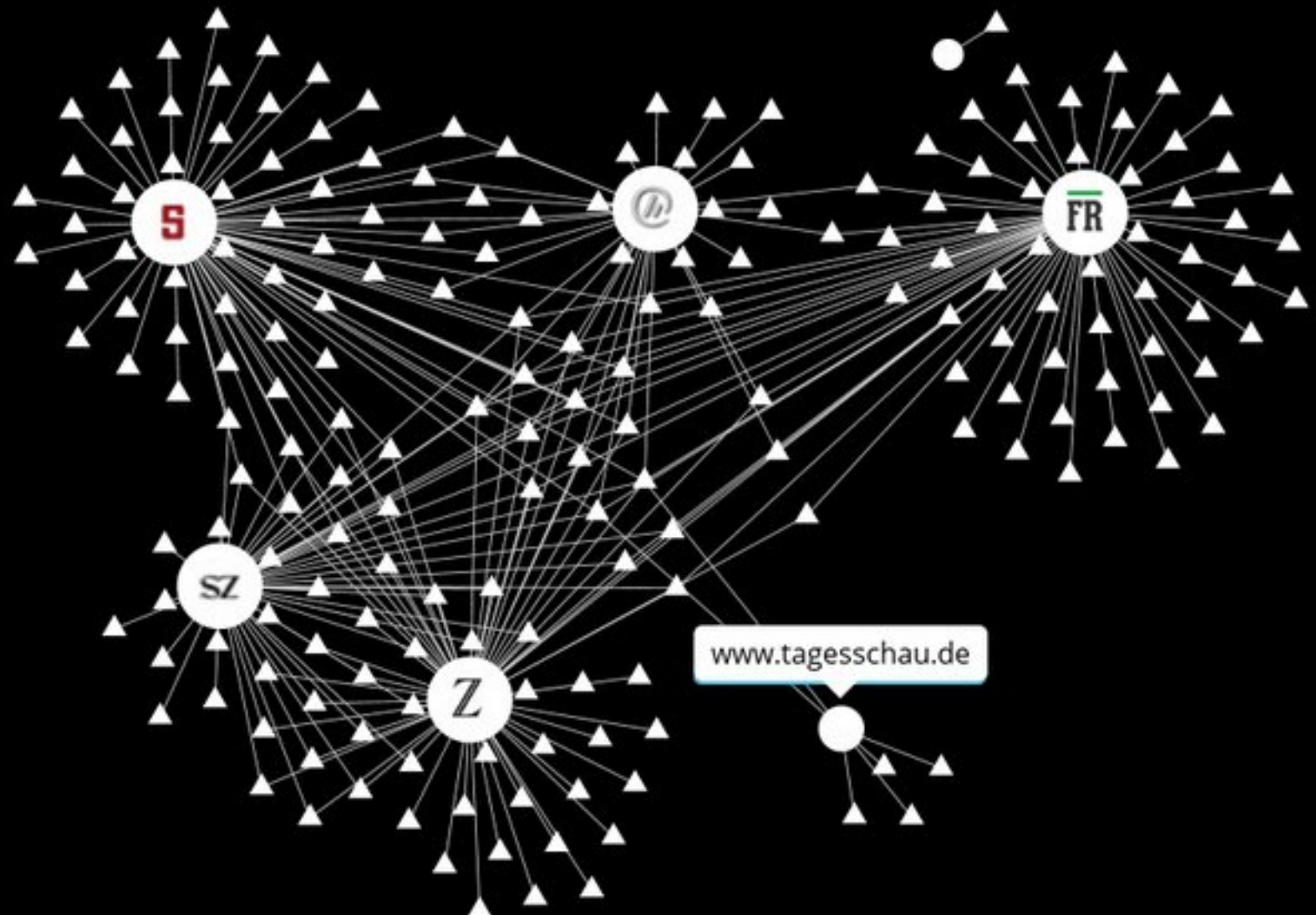
Save Data

Reset Data

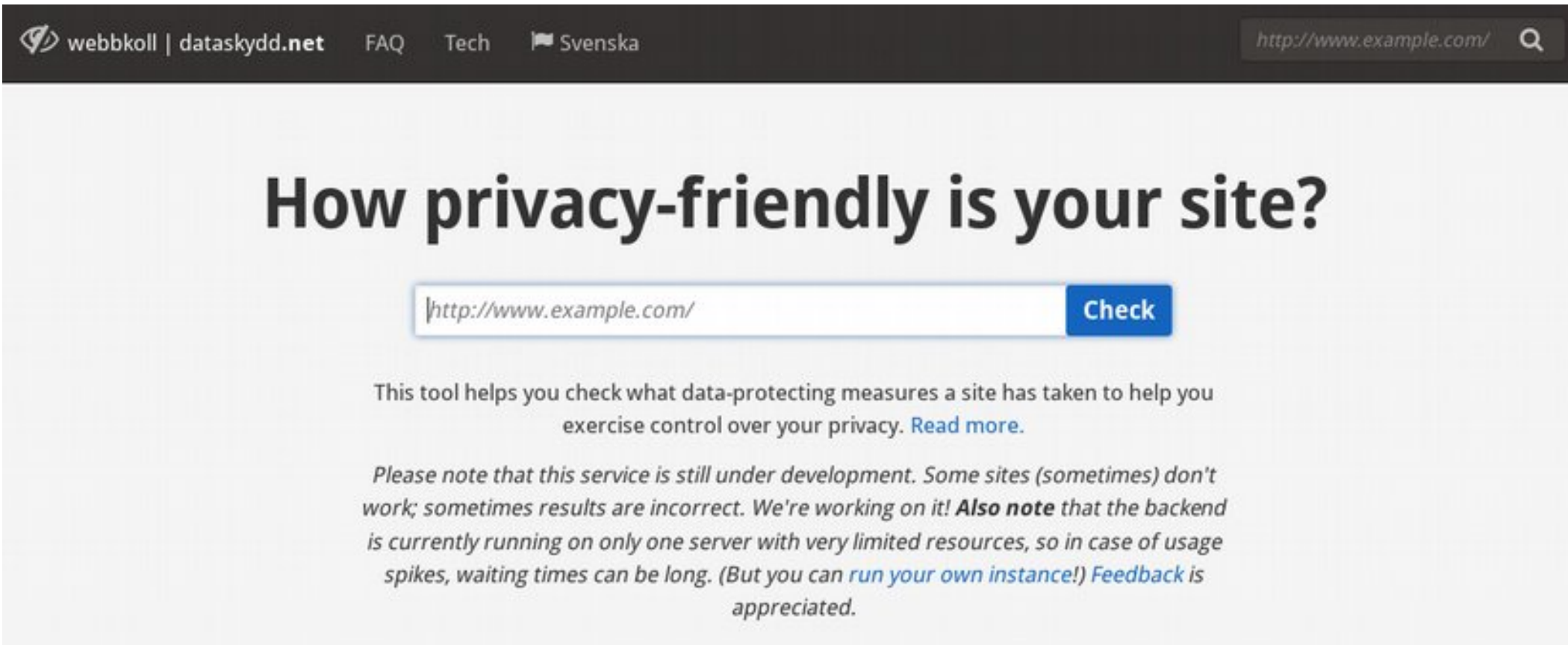
Give Us Feedback

Recent Site

GRAPH VIEW



Einfach selber testen mit Webbkoll



The screenshot shows the webbkoll website. The header is dark with the logo 'webbkoll | dataskydd.net' on the left, and links for 'FAQ', 'Tech', and 'Svenska' in the center. On the right, there is a search bar with the URL 'http://www.example.com/' and a magnifying glass icon. The main content area has a large heading 'How privacy-friendly is your site?'. Below this is a form with a text input field containing 'http://www.example.com/' and a blue 'Check' button. Under the form, there is a paragraph explaining the tool's purpose and a link to 'Read more'. A disclaimer follows, stating the service is under development and providing instructions on how to run a local instance, with a link for 'Feedback'.

webbkoll | dataskydd.net FAQ Tech Svenska <http://www.example.com/> 🔍

How privacy-friendly is your site?

[Check](#)

This tool helps you check what data-protecting measures a site has taken to help you exercise control over your privacy. [Read more.](#)

*Please note that this service is still under development. Some sites (sometimes) don't work; sometimes results are incorrect. We're working on it! **Also note** that the backend is currently running on only one server with very limited resources, so in case of usage spikes, waiting times can be long. (But you can [run your own instance!](#)) [Feedback](#) is appreciated.*

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

Sicheres Surfen mit Privatsphäre

Was wollen wir?

- Sicherheit:
 - Vertraulichkeit
 - Authentizität
 - Integrität
- Anonymität
 - Nur teilweise vereinbar mit Authentizität!
- Resistenz gegenüber Zensur

Wie bekommen wir das?

- HTTPS (Verschlüsselung)
- HTTPS (Zertifikate)
- HTTPS
- Firefox
- Tracking blocken
- Nur benötigte Cookies
- IP-Verschleierung

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.
- Eindeutiger Browser-Fingerabdruck:
 - <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**.

Wie kann ich mich vor Tracking schützen?

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

Firefox-Add-ons

- Tracker und Werbung blocken: **uBlock origin**
- Aktive Inhalte blocken: **NoScript**
- Scripts Globally Allowed (vom Hersteller nicht empfohlen)
- Webseiten immer verschlüsseln: **HTTPS Everywhere**
- Cookies automatisch löschen: **Cookie AutoDelete**
- Adobe-Flash am besten entfernen oder deaktivieren!
- Etwas komplizierter und aufwendiger:
- Alle Skripte blocken: **NoScript**
- Alle Drittanbieteranfragen blocken: **uMatrix**

Kontrolle

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

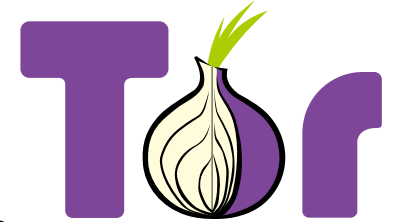
Weitere Firefox-Funktionen

- **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: The Onion Router
 - Netzwerk zur Anonymisierung von Verbindungsdaten
 - IP-Adresse wird verschleiert

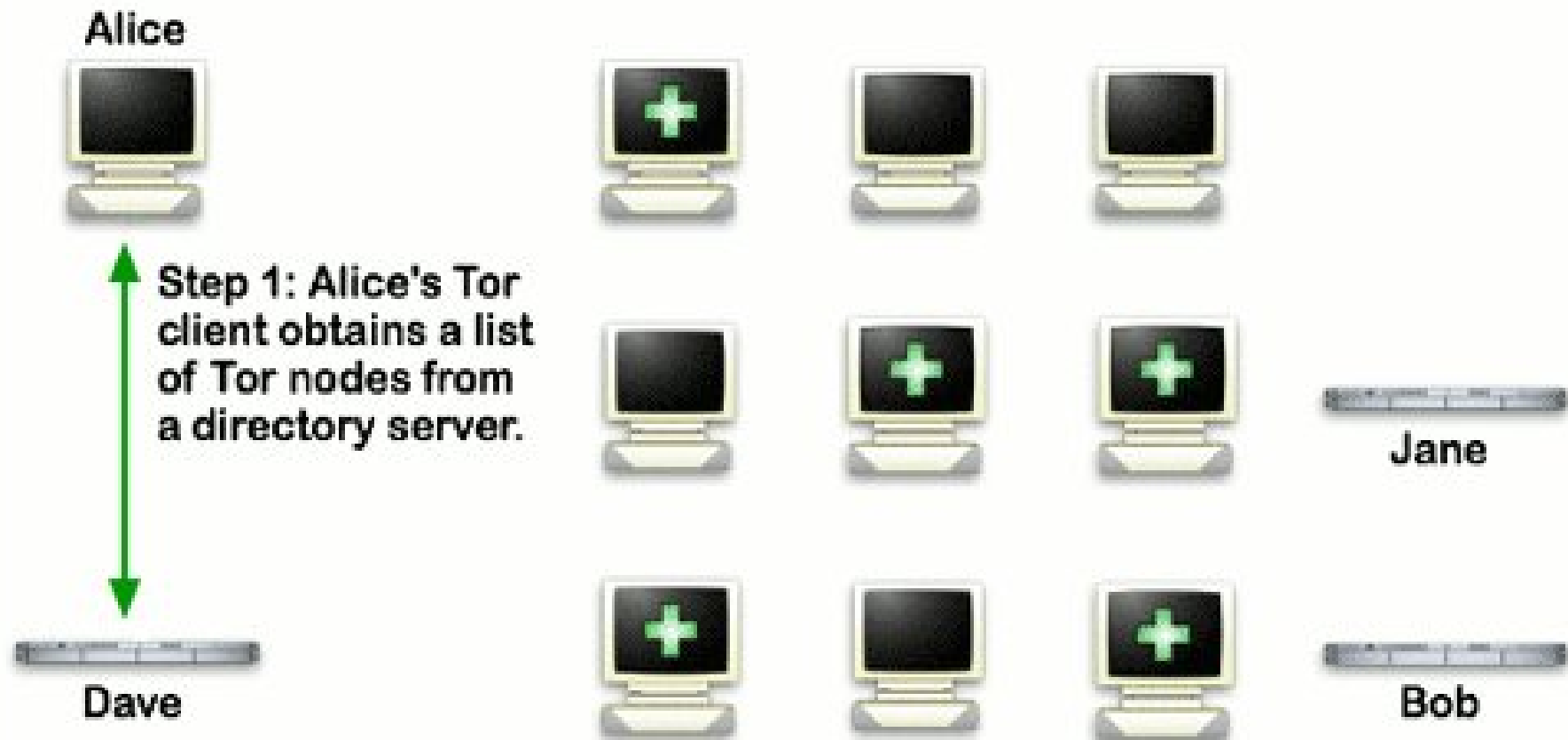
Vorteile

- Quelloffen, freie Software
- Anonymes Surfen

Nachteile

- Login bei personalisierten Seiten nicht sinnvoll
- Latenz ist größer

EE How Tor Works: 1



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.



Jane



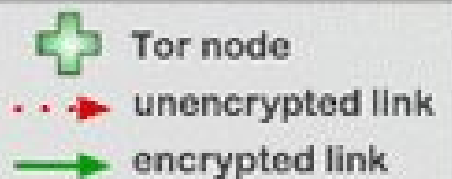
Dave



Bob



EE How Tor Works: 3



Alice



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



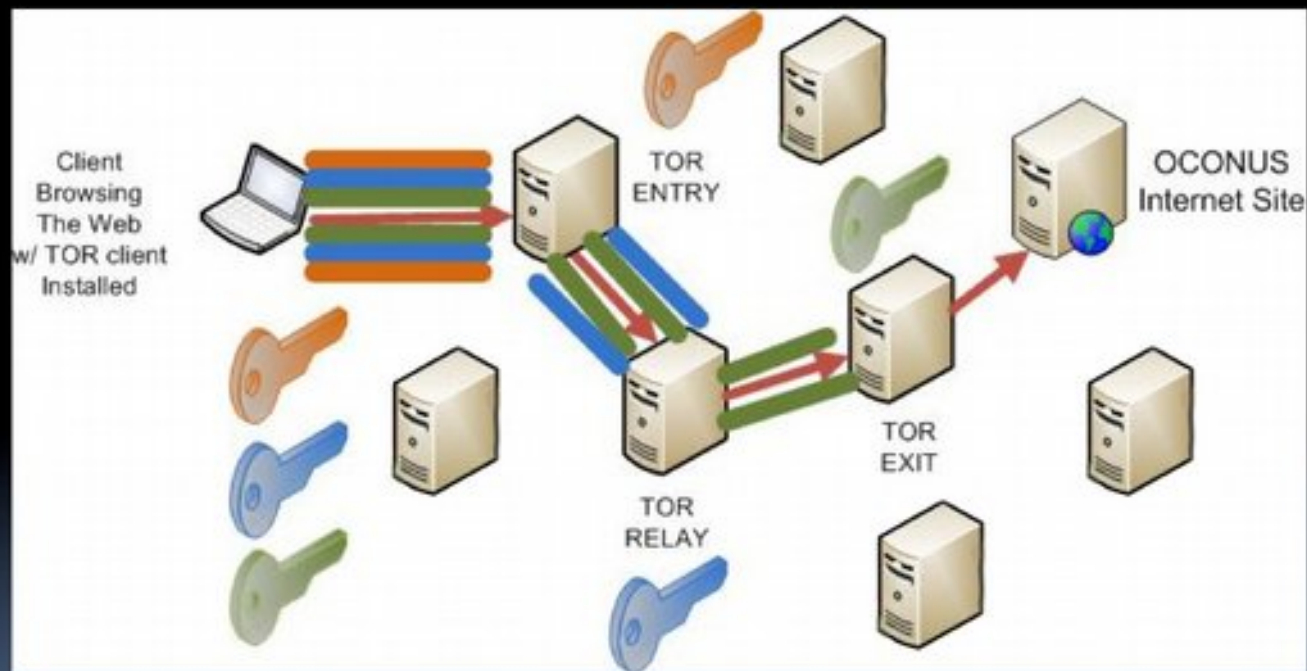
Jane



Bob

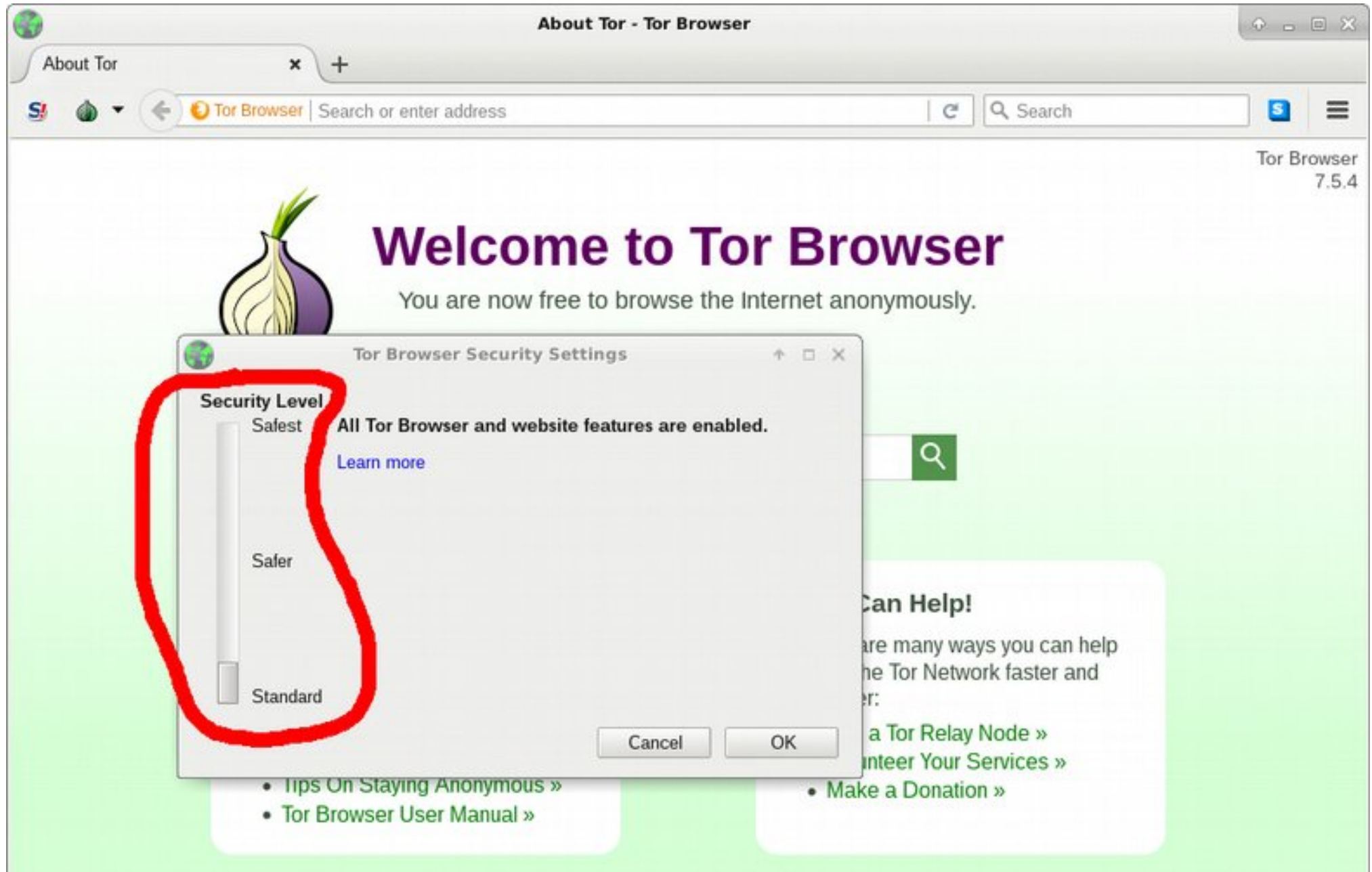


(U) What is TOR?



Download Tor-Browser

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



Tails – ein OS für Tor

- **The Amnesic Incognito Live System (Tails)**
- Live-Linux-DVD / USB
- Anonymität als erstes Designprinzip
- Viele Tools
 - Pidgin
 - Electrum
 - MAT
 - KeePassX

Weiterführende Literatur

- Das 3-Browser-Konzept von Mike Kuketz
<https://www.kuketz-blog.de/> (Stichwort "Not my data")
- Disconnect!- und Tails-Broschüre von Capulcu
<https://capulcu.blackblogs.org/neue-texte/>

Vielen Dank für's Mitmachen!



WebRTC (statt Skype)

- Firefox, Opera und Google Chrome
- Video-Telefonie **ohne Anmeldung**
- Aufbau durch Öffnen eines Links
- **Ende-zu-Ende-Verschlüsselung** mit **PFS**
- Keine starke Anonymität
- Läuft in der Amazon-Cloud
- Freie Software; eigenes Hosting möglich!
- **<https://meet.jit.si/>**

- Mittagspause -

E-Mail-Verschlüsselung

Alternativen zu „kostenlosen“ E-Mail-Anbietern

- **Posteo.de** oder **mailbox.org**
- 24h-Einmal-E-Mail-Adresse, gratis: anonbox.net (CA-Cert)

Vorteile

- Standort in Deutschland
- Datensparsamkeit
- Keine Inhaltsanalyse
- Keine Werbung
- Anonyme Nutzung möglich
- Datenschutz hat Priorität

Nachteile

- **posteo.de** und **mailbox.org**
kosten 1 € pro Monat

E-Mail-Verwaltung

- Software: **Mozilla Thunderbird**
 - Freie Software
 - Mehrere Mail-Konten möglich
 - Verwaltung mit Filtern und Ordnern
 - HTML abschalten möglich
 - Mails offline lesen, speichern und durchsuchen
 - Add-ons: Kalender, Massenmails, **Verschlüsselung**

Posteingang - test1@digitalcourage.de - Icedove

Posteingang - test1@di...

Abrufen ▾

Verfassen

Chat

Adressbuch

Schlagwörter ▾

Schnellfilter

Suchen... <Strg+K>

☰

test1@digitalcourage.de

Posteingang

cryptoseminiare

digitalcourage

Mailingliste1 (1)

Mailingliste2

test

Gesendet

Papierkorb

test2@digitalcourage.de

Posteingang (1)

Gesendet

Papierkorb

test3@digitalcourage.de

Posteingang (2)

Mailingliste1

Papierkorb

Lokale Ordner

Papierkorb

Postausgang

Archivierte Mails

✶	✎	Betreff	∞	Von	🕒	Datum	▼	Größe	📧
✶		Willkommen	•	georg test	•	15:47		0,9 KB	
✶		Ich bin weg...	•	test2@digitalcourage....	•	15:48		1,0 KB	

↩ Antworten

➡ Weiterleiten

📁 Archivieren

🗑 Junk

🗑 Löschen

Mehr ▾

Von Mir <test2@digitalcourage.de> ✨

Betreff **Ich bin weg...** 15:48

An Mich <test1@digitalcourage.de> ✨

Ich bin vom <date> bis <date> nicht zu Hause / im Büro.
 In dringenden Fällen setzen Sie sich bitte mit <contact person> in Verbindung.
 Vielen Dank für Ihr Verständnis.

Ungelesen: 0

Gesamt: 2


digitalcourage
 Hochschulgruppe

E-Mail-Verschlüsselung (PGP / GnuPG)

Vorteile

- Inhalt Ende-zu-Ende-verschlüsselt
- Absender¹ & Empfängerin werden eindeutig
(¹ mit PGP-Signatur)

Nachteile

- Metadaten (von, an, Betreff² etc). bleiben unverschlüsselt
(² Enigmail ab 2.0 kann Betreff verschlüsseln)
- Absender & Empfängerin müssen PGP nutzen

Benötigte Software:

- E-Mail Programm: Thunderbird
- Add-on: **Enigmail**
 - **p≡p** (Pretty Easy Privacy) nutzen wir noch nicht (ggf. deaktivieren)

Verschlüsselung – was ist das eigentlich?

- Alice schreibt an Bob, Eve will mithören (eavesdrop) / Mallory (malicious) will manipulieren → man in the middle
- Beispiele und Grundprinzipien
 - meist gibt es ein **Verfahren** mit **Schlüssel**
 - Caesar-Verschlüsselung: einheitliche Verschiebung, 3 Positionen – wurde tatsächlich von Caesar und lange danach eingesetzt
 - ab 16. Jahrhundert komplexere Verfahren, noch im 1. Weltkrieg handschriftlich, 2. Weltkrieg Enigma – entscheidende Misserfolge
 - Vertrauen in moderne Kryptographie beruht darauf, dass das **Verfahren offen**, der **Schlüsselraum sehr groß** und als Angriff eigentlich **nur brute force** (alle Schlüssel probieren) bekannt ist

Unterschied symmetrische / asymmetrische Verschlüsselung

Symmetrische Verschlüsselung

- **Derselbe Schlüssel** zum Ver- und Entschlüsseln
- Alle Beteiligten brauchen diesen (geheimen) Schlüssel
- Problem: um Nachrichten (auf unsicheren Kanälen) zu senden, muss zuerst der Schlüssel (auf sicherem Kanal) verteilt werden

Unterschied symmetrische / asymmetrische Verschlüsselung

Asymmetrische Verschlüsselung → PGP

- **Schlüsselpaar:** was **ein** Schlüssel **verschlüsselt**, muss mit dem **anderen** Schlüssel **entschlüsselt** werden
- Alle Beteiligten erzeugen ein eigenes Schlüsselpaar
- Öffentlicher Schlüssel
 - kann und muss verteilt werden (an alle, über unsichere Kanäle)
- Privater Schlüssel
 - bleibt privat – gut schützen und sichern, niemals herausgeben!
- Zentrale Voraussetzungen
 - private Schlüssel können von niemand sonst benutzt werden
 - öffentliche Schlüssel sind unverfälscht und korrekt zugeordnet

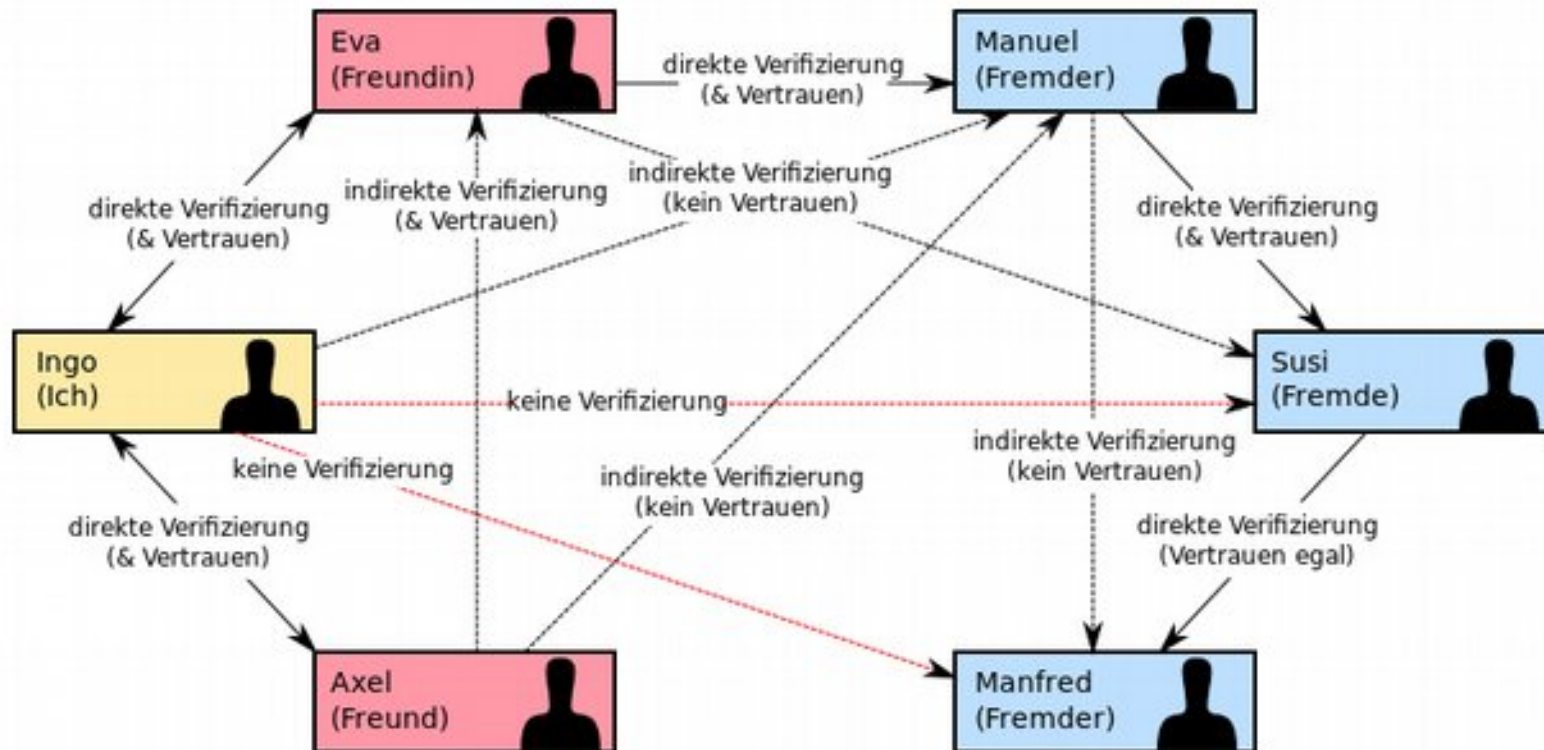
E-Mails verschlüsseln und signieren

- Verschlüsseln
 - sichert Vertraulichkeit der Nachricht
 - verwendet den **öffentlichen Schlüssel des Empfängers**
(nur der Empfänger kann mit privatem Schlüssel entschlüsseln)
- Signieren
 - sichert Unverfälschtheit der Nachricht und wer sie verfasste
 - nicht verwechseln mit Unterschrift und Fußzeile („Signatur“)
 - ein Fingerabdruck der Nachricht wird verschlüsselt und angehängt
 - verwendet den **privaten Schlüssel der Absenderin**
(niemand anders konnte diesen Schlüssel einsetzen)
- Verschlüsseln und Signieren sind unabhängig voneinander

öffentliche PGP-Schlüssel austauschen

- E-Mail-Anhang
 - zur Verteilung im privaten Kreis
- Key-Server
 - bequem durchsuchbar
 - E-Mail-Adresse öffentlich einsehbar
- Habe ich den richtigen Schlüssel bekommen?
 - komplexes Thema → Schlüssel signieren, „Web of Trust“
 - pragmatische Lösung: Schlüssel auf mehreren Wegen finden (z.B. von persönlicher Website); Fingerprints austauschen und vergleichen (Visitenkarte, Telefon, Website, „Signatur“ unter Mails)

Web of Trust



CC-BY-SA Ogmios (Wikimedia Commons)

Posteingang - test1@digitalcourage.de - Icedove

Posteingang - test1@di...

Abrufen ▾ Verfassen Chat Adressbuch Schlagwörter ▾ Schnellfilter Suchen... <Strg+K>

test1@digitalcourage.de

- Posteingang
 - cryptoseminiare
 - digitalcourage
 - Mailingliste1 (1)
 - Mailingliste2
 - test
 - Gesendet
 - Papierkorb
- test2@digitalcourage.de
 - Posteingang (1)
 - Gesendet
 - Papierkorb
- test3@digitalcourage.de
 - Posteingang (2)
 - Mailingliste1
 - Papierkorb
- Lokale Ordner
 - Papierkorb
 - Postausgang
 - Archivierte Mails

	Betreff	Von	Datum	Größe
☆	Willkommen	georg test	15:47	0,9 KB
☆	Ich bin weg...	test2@digitalcourage....	15:48	1,0 KB

Verfassen: verschlüsselte Mail

Datei Bearbeiten Ansicht Optionen Enigmail Extras Hilfe

Senden Rechtschr. ▾ Anhang ▾ S/MIME ▾ Speichern ▾

Enigmail: Meinen öffentlichen Schlüssel anhängen Nachricht wird unterschrieben und verschlüsselt.

Von: georg test <test1@digitalcourage.de> test1@digitalcourage.de

An: test3@digitalcourage.de

An:

Betreff: verschlüsselte Mail

Hallo Test3,
endlich habe ich mir Verschlüsselung eingerichtet ...

Ungelesen: 0 Gesamt: 2

- Kleine Praxis -

Mobilgeräte

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...

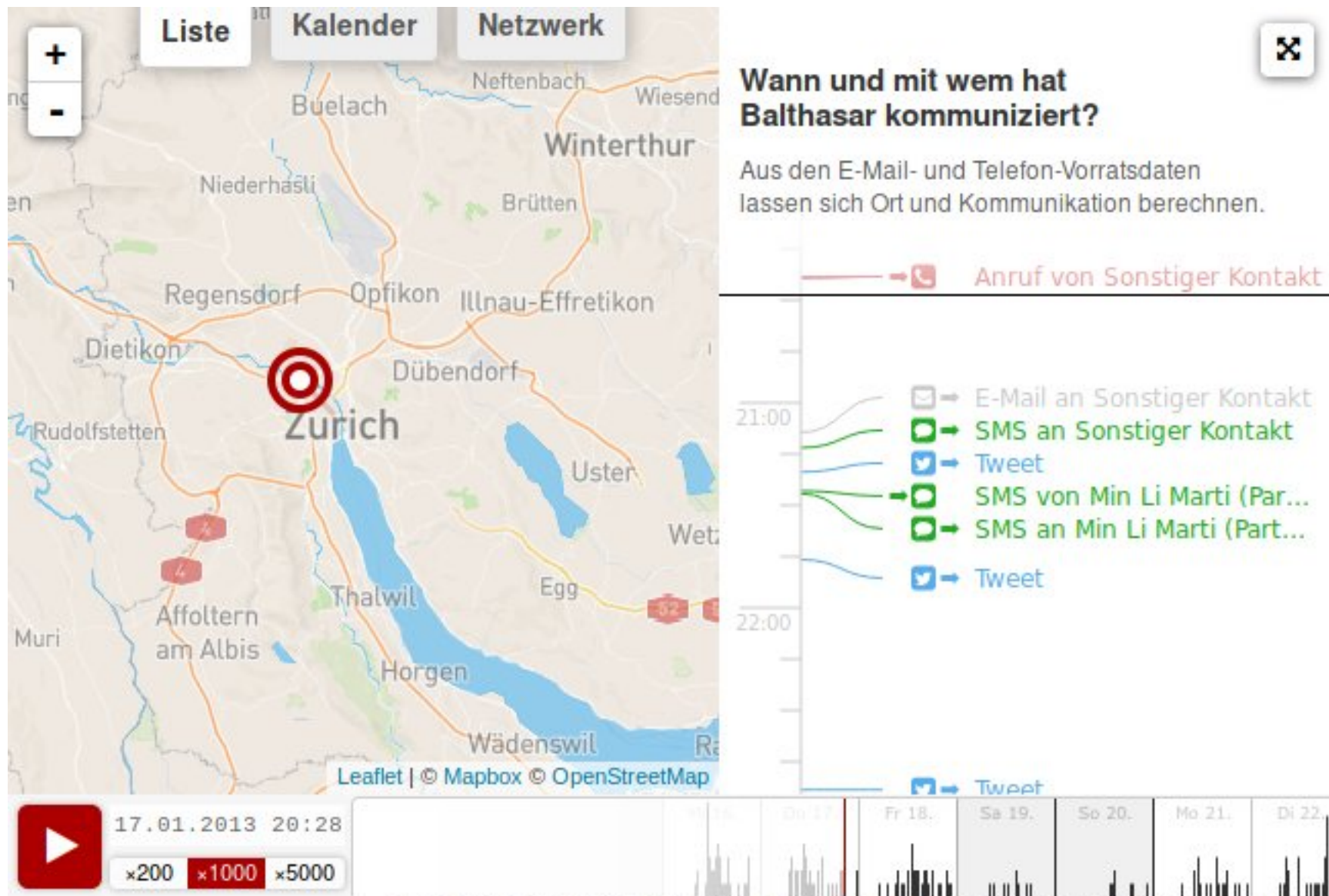
(Kontaktbeziehungen, Reisedaten, Finanztransfers, ...)

- ...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 Telefon



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)

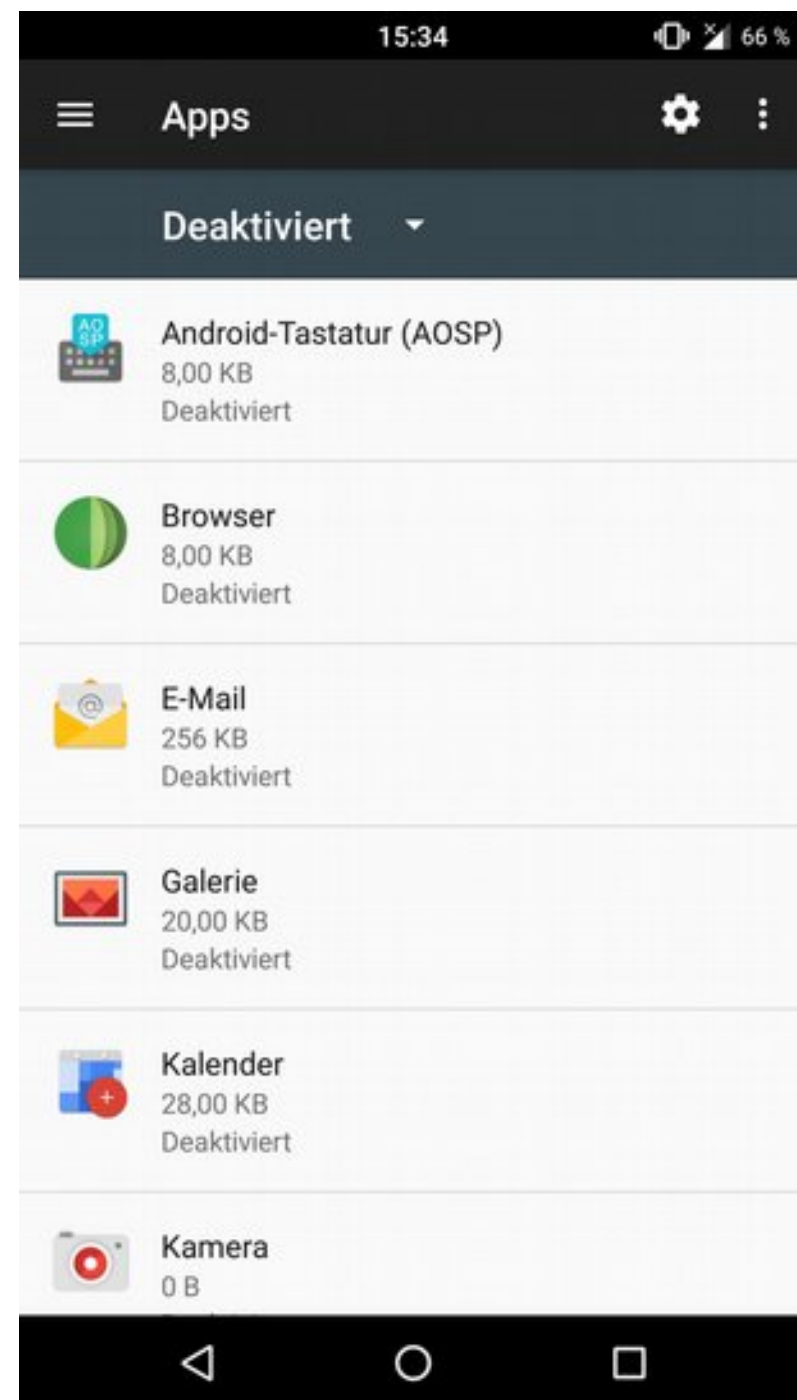
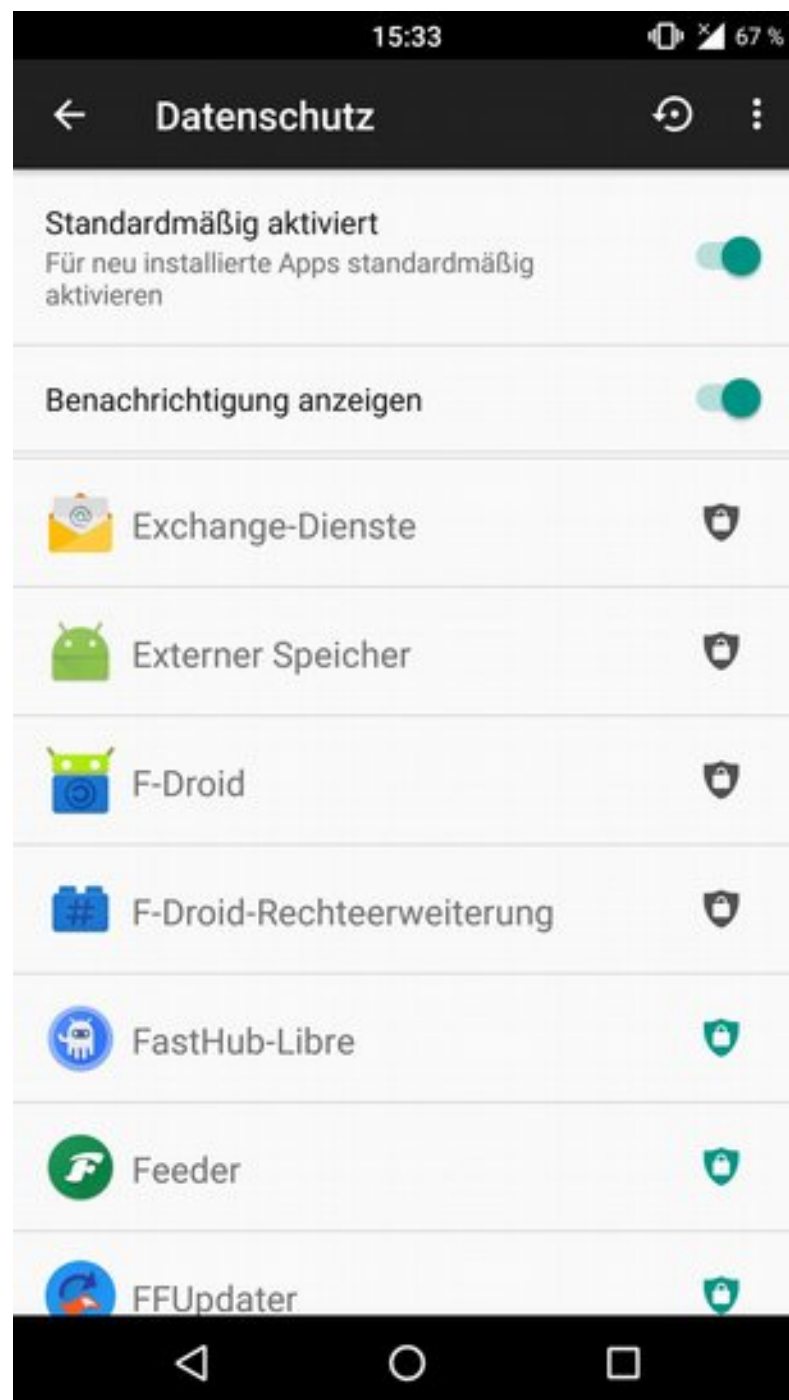
- Kamera
 - Bilder und Videos aufzeichnen
- Mikrofon
 - Ton aufzeichnen
- WLAN-Verbindungsinformationen
 - WLAN-Verbindungen abrufen
- Geräte-ID & Anrufinformationen
 - Telefonstatus und Identität

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.



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

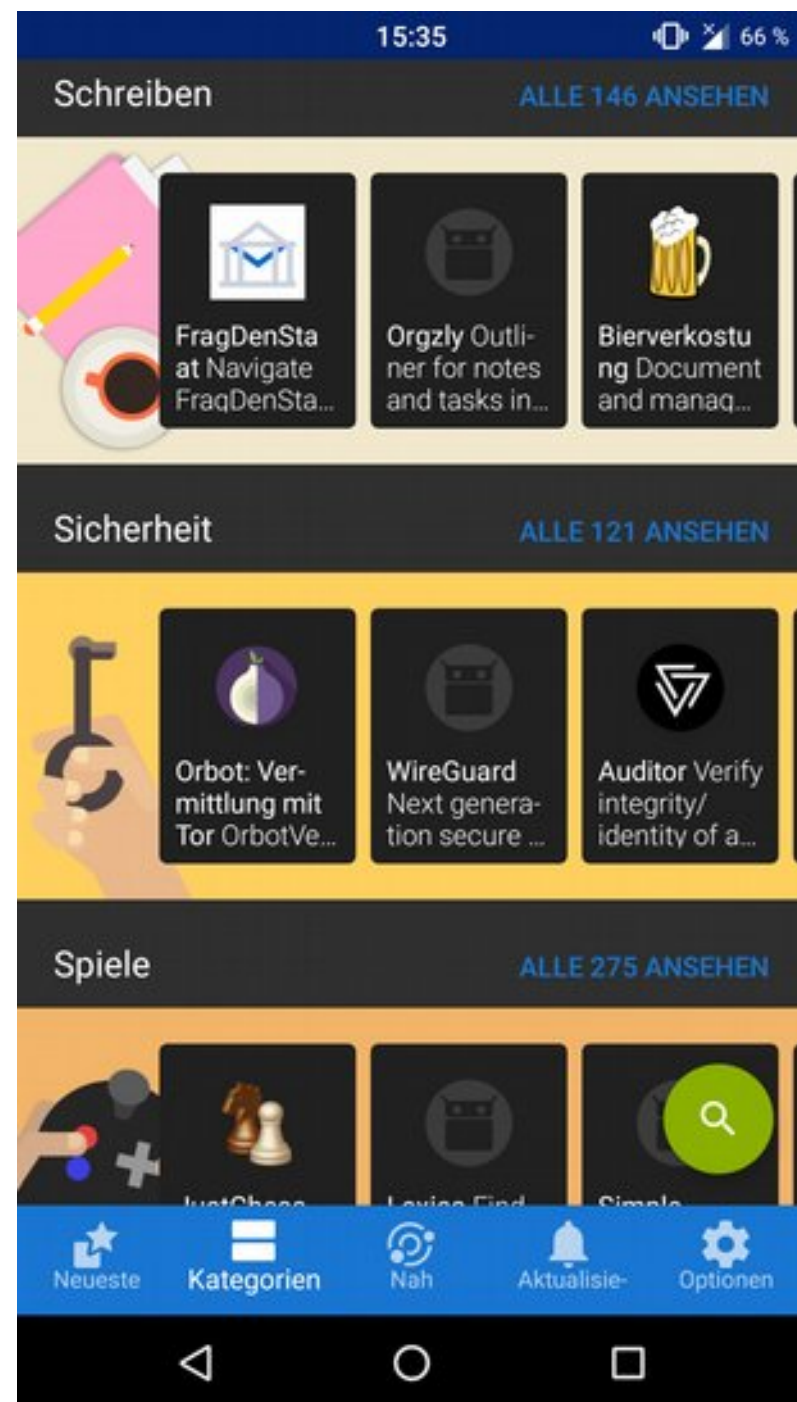
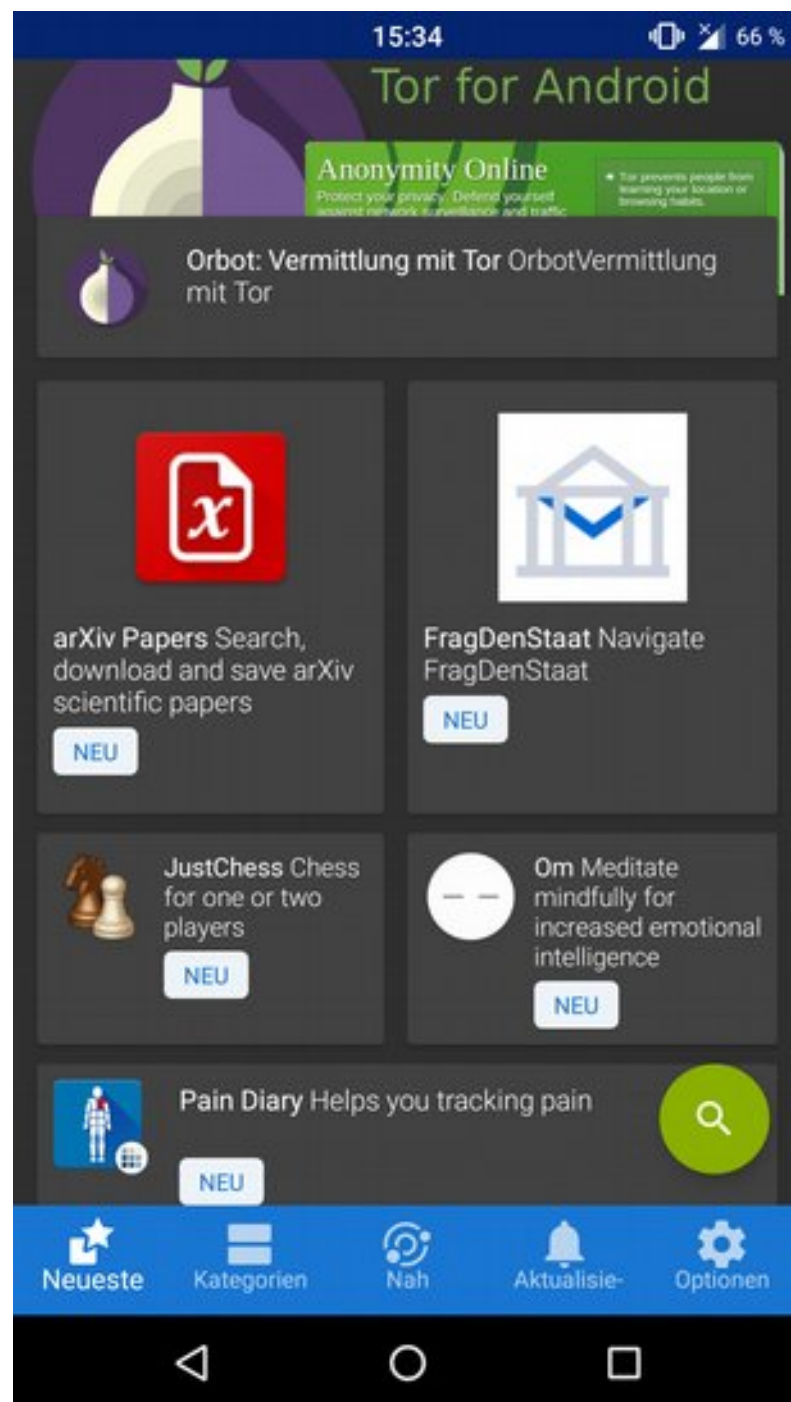
4. Freie Android-Variante installieren

- 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)





Ansprüche an Messenger

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

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 Verschlüsselungsalgorithmus
- 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



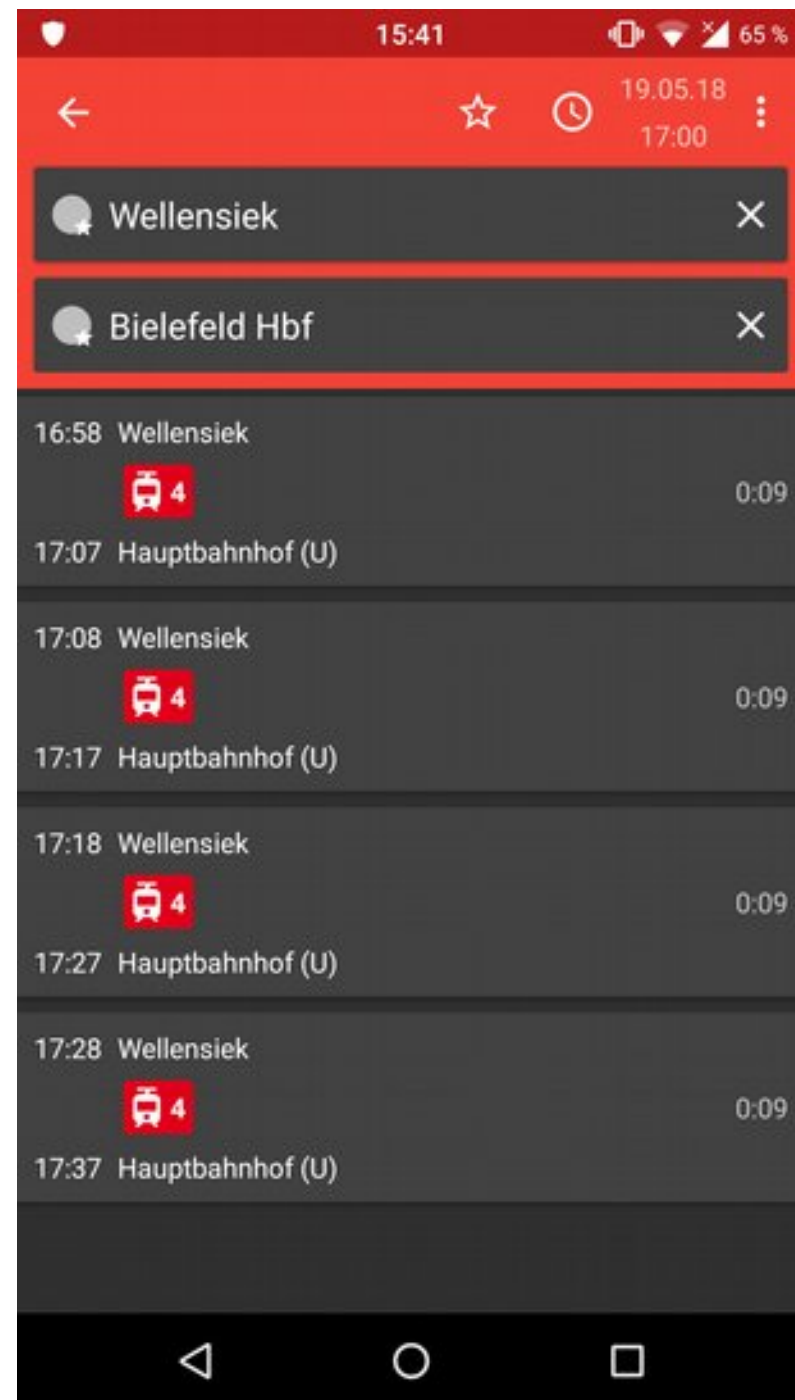
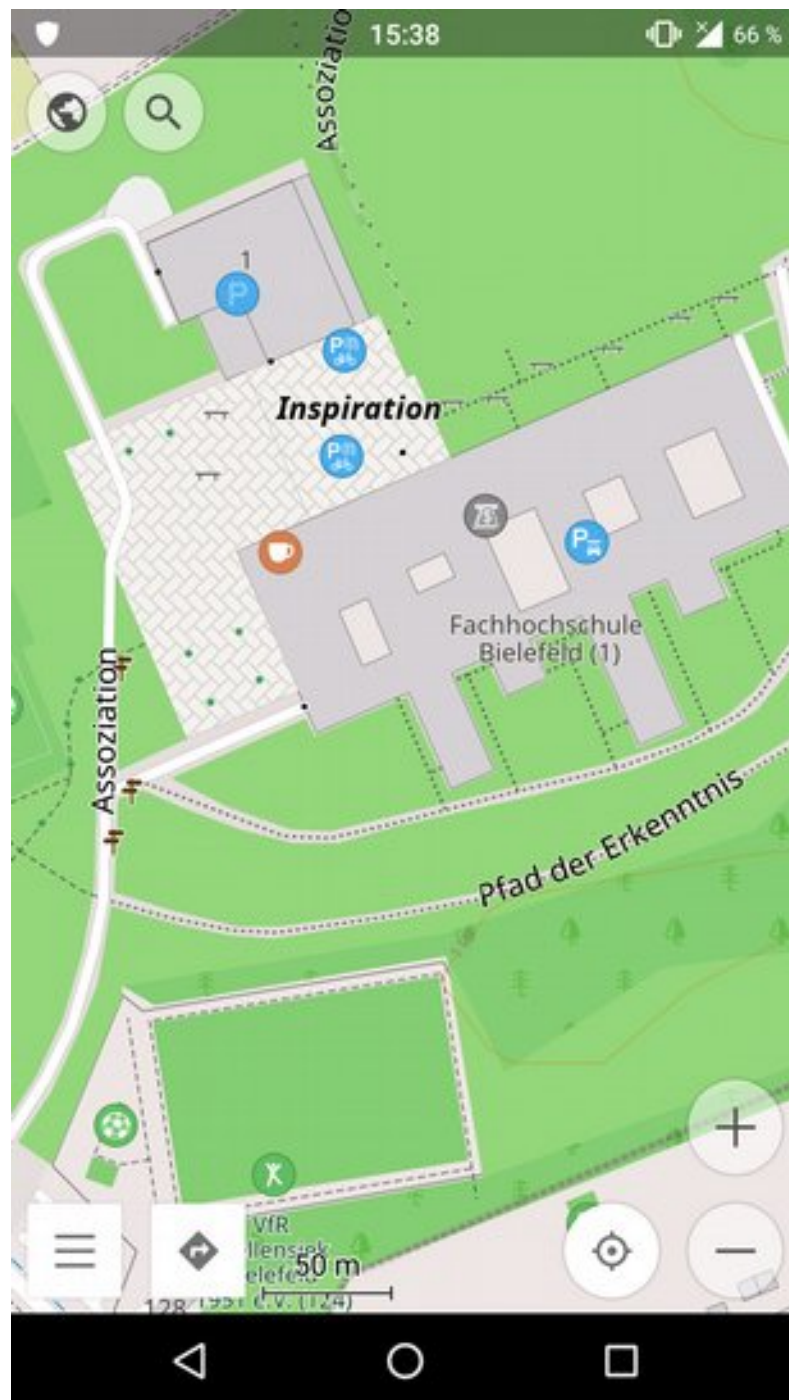
- **VLC**

- Video- und Audioplaye



- **OsmAnd+**

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



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/>

Anlaufstellen in Bielefeld

- **Digitalcourage e.V.**

- Wöchentliches Kennenlernetreffen jeden Dienstag um 20 Uhr im Grec Tavernio (Niederwall 23).
- <https://digitalcourage.de/treffen-vor-ort>

- **Digitalcourage-Hochschulgruppe**

- Trifft sich jeden ersten und dritten Montag im Monat um 18 Uhr im SozCafé (X-C2-116)
- <https://digitalcourage.de/hsg>

Vielen Dank
für die Aufmerksamkeit

Fragen?!

- Praxis -