Digitale Selbstbestimmung für EinsteigerInnen

Sylvia Lange

Cryptoparty Tübingen 22.7.2023

Fragen?

- Es gibt keine dummen Fragen!
- Verständnisfragen bitte direkt.
- Alle anderen Fragen im Anschluss an den Vortrag.

Sylvia Lange

- Lehrerin für Informatik (Oberstufe am Beruflichen Gymnasium)
- Engagiert im Chaos Computer Club
- Beschäftigung mit Datenschutzthemen in der Freizeit, z.B. bei Events des CCC

Disclaimer

- Die Autorin ist weder IT-Sicherheits-Expertin noch Juristin.
- Manche der Informationen veralten schnell.

Begriffsklärung – zwei Arten von Schutzzielen

Umweltschutz,
Artenschutz,
Informantenschutz,
Jugendschutz,
Mutterschutz,
Landschaftsschutz

Virenschutz,
Sonnenschutz,
Lärmschutz,
Feuerschutz,
Erosionsschutz,
Kälteschutz,
Wärmeschutz
Hochwasserschutz,
Kündigungsschutz,
Blitzschutz

Was ist Datenschutz?

Datenschutz ist nicht der Schutz **von Daten**, sondern der Schutz **von Menschen vor dem Missbrauch von Daten**.

Regeln, die älter als die Digitalisierung sind

Warum darf ein Arbeitgeber beim Bewerbungsgespräch nicht nach der Familienplanung fragen?

Warum gibt es die ärztliche Schweigepflicht?

Regeln, die älter als die Digitalisierung sind

Bewerbungsgespräch

- Schutz vor Diskriminierung
- Nachteile von Erziehungszeiten sollen **solidarisch** getragen werden.

ärztliche Schweigepflicht

- Schutz vor Stigmatisierung / Diskriminierung
- geschützter Rahmen ermöglicht erst das Hilfeholen

Missbrauchspotenzial durch Daten

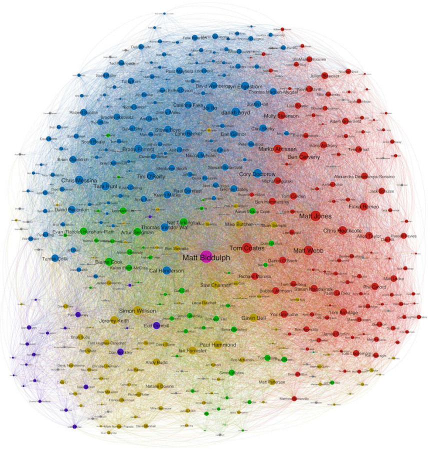
- Diskrimierung (z.B. Arbeitsmarkt, Preisdiskriminierung, Preise für Versicherungen)
- Manipulation (z.B. Microtargeting, bei Wahlen, siehe Cambridge Analytica)
- Unterdrückung von Opposition
- ungesunde Marktmacht (z.B. Thema KI und autonomes Fahren)

Video von mobilsicher zu den Gründen für Datenschutz:
`https://peertube.mobilsicher.de/w/qjKXZJfij9wVvBQscMbcqy`

Problem der Datenhäufung

- Größere Datensammlungen sind mehr als die Summe der Einzelteile.
  Aus vielen, vielen an sich harmlosen Daten setzt sich ein Gesamtbild der Persönlichkeit und des Gesundheitszustandes zusammen.
- Große Datensammlungen sind ein **Marktvorteil**. Ein kleines Startup könnte nie eine KI für autonomes Fahren bauen.

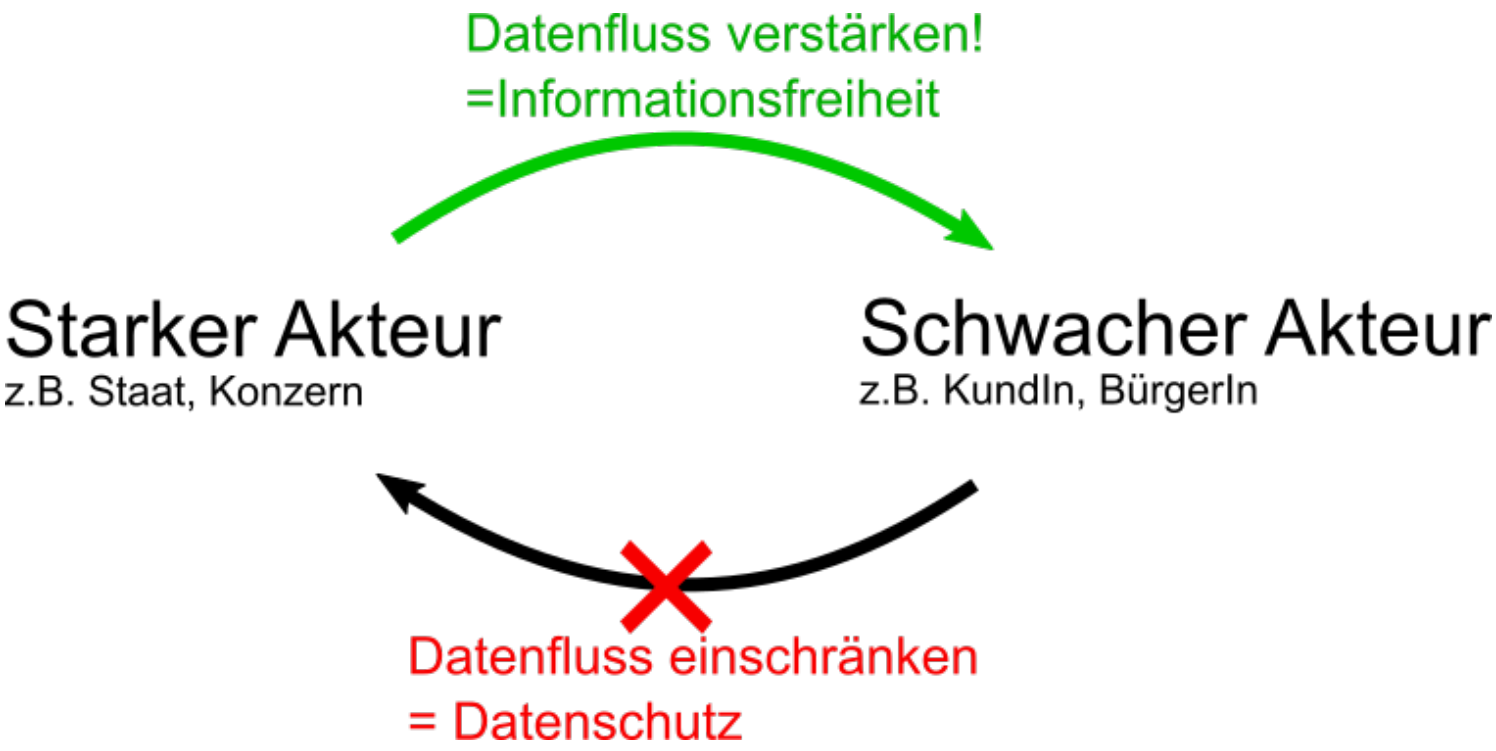
Gefahren eines umfassenden Social Graphs



Gefahren eines umfassenden Social Graphs

- gezielte politische Einflussnahme und Manipulation
- gezielte Manipulation der öffentlichen Meinung, Desinformation
- Social Engineering Angriffe
- Betrug und Identitätsdiebstahl

Datenschutz und Informationsfreiheit



Recht auf Informationsfreiheit nutzen

- Internet-Plattform zur Erleichterung von Anfragen an Behörden und Institution **FragDenStaat**
  `https://fragdenstaat.de/`
- Projekt der Open Knowledge Foundation Deutschland
  `https://okfn.de/`

Gegenmaßnahmen „am Gerät“

- bestimmte Dienste meiden
- insbesondere Dienste meiden, die Zustimmung zu langen und unverständlichen AGB verlangen
- Ende-zu-Ende-Verschlüsselung nutzen!

ABER: Der Schutz auf Userseite hat deutliche Grenzen! Schutz der Bürger durch Politik nötig!

Politische Gegenmaßnahmen: Die DSGVO

- DSGVO = Datenschutzgrundverordnung der EU
- politischer Durchbruch wegen **Marktortprinzip:**
  Es gelten die Gesetze der EU, wenn ein Produkt in der EU angeboten wird. Egal wo der Firmensitz des Unternehmens ist.
- sehenswerte Reportage über den politischen Prozess auf EU-Ebene: *Democracy - Im Rausch der Daten*, David Bernet
- **Problem:** geltendes Recht muss durchgesetzt werden, siehe BBA 2022 für Irische Datenschutzbehörde.

  `https://bigbrotherawards.de/`
- Schützt Bürger, Konsumenten, **ABER** nur bis zur Zustimmung zu AGB!

Politische Gegenmaßnahmen: Die DSGVO

- DSGVO = Datenschutzgrundverordnung der EU
- politischer Durchbruch wegen **Marktortprinzip:**
  Es gelten die Gesetze der EU, wenn ein Produkt in der EU angeboten wird. Egal wo der Firmensitz des Unternehmens ist.
- sehenswerte Reportage über den politischen Prozess auf EU-Ebene: *Democracy - Im Rausch der Daten*, David Bernet
- **Problem:** geltendes Recht muss durchgesetzt werden, siehe BBA 2022 für Irische Datenschutzbehörde.

  `https://bigbrotherawards.de/`
- Schützt Bürger, Konsumenten, **ABER** nur bis zur Zustimmung zu AGB!

Politische Gegenmaßnahmen: Die DSGVO

- DSGVO = Datenschutzgrundverordnung der EU
- politischer Durchbruch wegen **Marktortprinzip:**
  Es gelten die Gesetze der EU, wenn ein Produkt in der EU angeboten wird. Egal wo der Firmensitz des Unternehmens ist.
- sehenswerte Reportage über den politischen Prozess auf EU-Ebene: *Democracy - Im Rausch der Daten*, David Bernet
- **Problem:** geltendes Recht muss durchgesetzt werden, siehe BBA 2022 für Irische Datenschutzbehörde.

  `https://bigbrotherawards.de/`
- Schützt Bürger, Konsumenten, **ABER** nur bis zur Zustimmung zu AGB!

Politische Gegenmaßnahmen: Die DSGVO

- DSGVO = Datenschutzgrundverordnung der EU
- politischer Durchbruch wegen **Marktortprinzip:**
  Es gelten die Gesetze der EU, wenn ein Produkt in der EU angeboten wird. Egal wo der Firmensitz des Unternehmens ist.
- sehenswerte Reportage über den politischen Prozess auf EU-Ebene: *Democracy - Im Rausch der Daten*, David Bernet
- **Problem:** geltendes Recht muss durchgesetzt werden, siehe BBA 2022 für Irische Datenschutzbehörde.

  `https://bigbrotherawards.de/`
- Schützt Bürger, Konsumenten, **ABER** nur bis zur Zustimmung zu AGB!

Politische Gegenmaßnahmen: Die DSGVO

- DSGVO = Datenschutzgrundverordnung der EU
- politischer Durchbruch wegen **Marktortprinzip:**
  Es gelten die Gesetze der EU, wenn ein Produkt in der EU angeboten wird. Egal wo der Firmensitz des Unternehmens ist.
- sehenswerte Reportage über den politischen Prozess auf EU-Ebene: *Democracy - Im Rausch der Daten*, David Bernet
- **Problem:** geltendes Recht muss durchgesetzt werden, siehe BBA 2022 für Irische Datenschutzbehörde.

  `https://bigbrotherawards.de/`
- Schützt Bürger, Konsumenten, **ABER** nur bis zur Zustimmung zu AGB!

DSGVO und AGB

Merke: Ab dem Moment, wo der Kunde zu etwas zustimmt, ist alles legal wozu die Einwilligung gegeben wurde.
DSGVO-konform heißt nur: Der Kunde hat allem, was passiert, zugestimmt.
DSGVO-konform $\neq$ datensparsam

DSGVO in Kurzform

- Recht auf Auskunft
- Zweckbindung
- Datenminimierung (nur notwendige Daten)
- „Recht auf Vergessen“
- Integrität (Daten sachlich richtig) und Vertraulichkeit (Dritte haben keinen Zugriff)

Prinzip der Zustimmung des Individuums: **Muss in Zeiten von KI überdacht werden!!**

DSGVO: Zustimmungsprinzip nicht mehr zeitgemäß!

Training einer KI

vermeintlich harmlose Daten, von UserInnen geteilt

z.B. Spotify Hörverlauf

→ heikle Daten, von UserInnen geteilt

z.B. politische Einstellungen, Erkrankungen, sexuelle Orientierung

Vorhersage mit KI

vermeintlich harmlose Daten, von anderen UserInnen geteilt

z.B. Spotify Hörverlauf

→ Informationen, die bewusst **nicht** geteilt wurden

z.B. politische Einstellungen in autoritärem Staat

Siehe `https://predictiveprivacy.org/`

Kollektive Dimension des Datenschutzes

- Aufgrund Daten anderer sind Vorhersagen über mich möglich. (sogar auch mit anonymisierten Daten)
- Meine Daten gefährden andere.
- Deshalb gilt: „Datenschutz ist ein **Team**sport.“
- Marktprinzipien versagen hier genauso wie beim Umweltschutz.

Eine sinnvolle politische Forderung: Interoperabilität

- WhatsApp kann nicht mit Signal „reden“
- Der Gesetzgeber könnte genau diese Interoperabilität fordern
- Die Quasi-Monopolstellung von WhatsApp wäre gebrochen

Organisationen unterstützen!

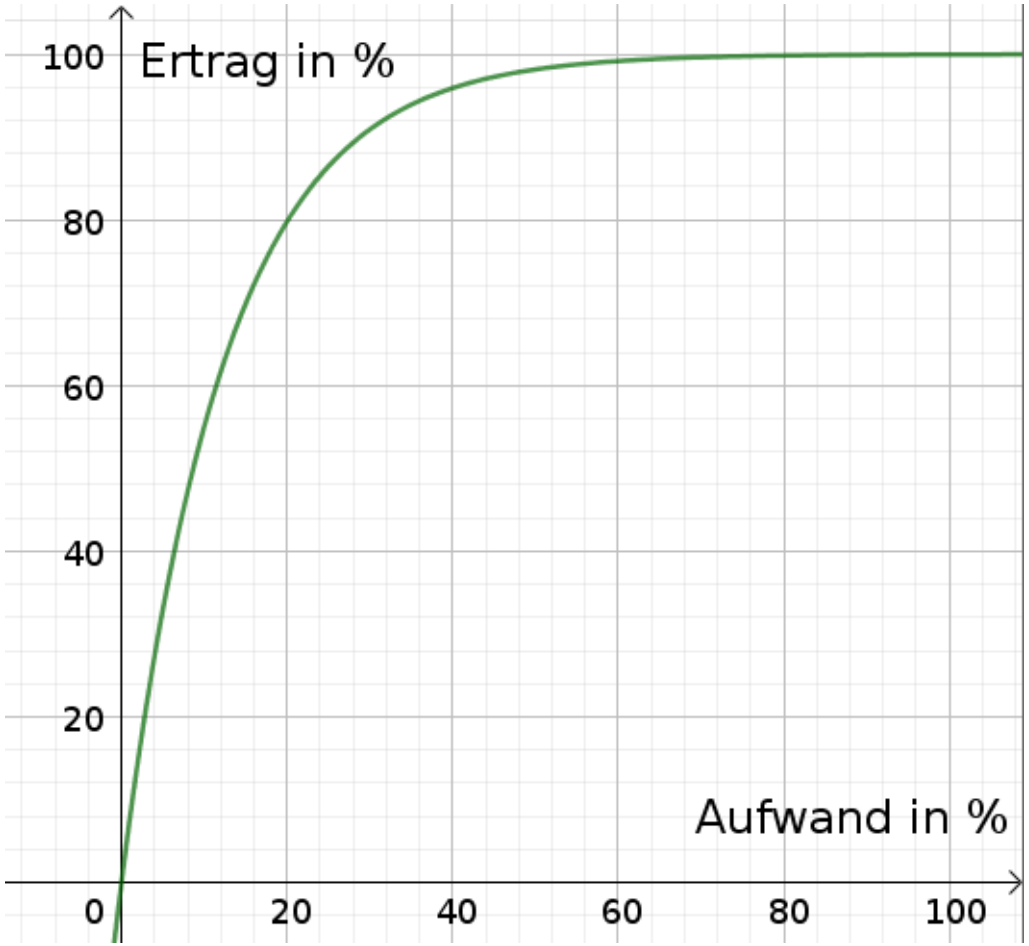
Digitalcourage, Electronic Frontier Foundation (EFF) Deutschland, Digitale Gesellschaft, EDRI, noyb, ...

- machen Lobby-Arbeit, kleiner aber wichtiger Gegenpol zu Lobbyisten von Big Tech
- reisen nach Brüssel, sprechen mit Politikern
- informieren die Öffentlichkeit, z.B. Big Brother Award (von Digitalcourage)
- **sind auf Spenden angewiesen**

Politische Arbeit versus Maßnahmen des Individuums

- Man kann sich nicht komplett gegen Datenabfluss schützen, es sei denn man zieht in den Wald oder eine Höhle und verzichtet komplett auf Technik.
- Man kann aber den Datenabfluss reduzieren.
- Die wichtigste Ebene ist aber die Politische!

Meine Empfehlung: Pareto



Meine ganz persönliche Empfehlung

Pareto: Den eigenen Datenabfluss mit **vertretbarem** Aufwand auf 20% reduzieren. Lieber regelmäßig für Datenschutz- Organisationen **spenden** als einen großen Aufwand für Individualmaßnahmen betreiben.

Sich deprimiert fühlen hilft nicht. Spenden aber wohl.

Was die einzelne UserIn am Gerät tun kann

Digitale Selbsterverteidigung

- faire Messenger benutzen
- datensparsam Surfen (3-Browser-Konzept)
- faire Dienste nutzen
- Freie OpenSource-Software nutzen

Messenger

Whatsapp meiden!

- gehört zu Meta (Facebook-Konzern), also Problem der **Datenhäufung**
- Meta kann zwar (vermutlich) nicht den Nachrichten- Inhalt lesen, aber **Metadaten** verraten bereits sehr viel
- **Kontakte** werden zu Meta hochgeladen. Meta hat den größten **Social Graph** der Welt.

Messenger

Signal Messenger

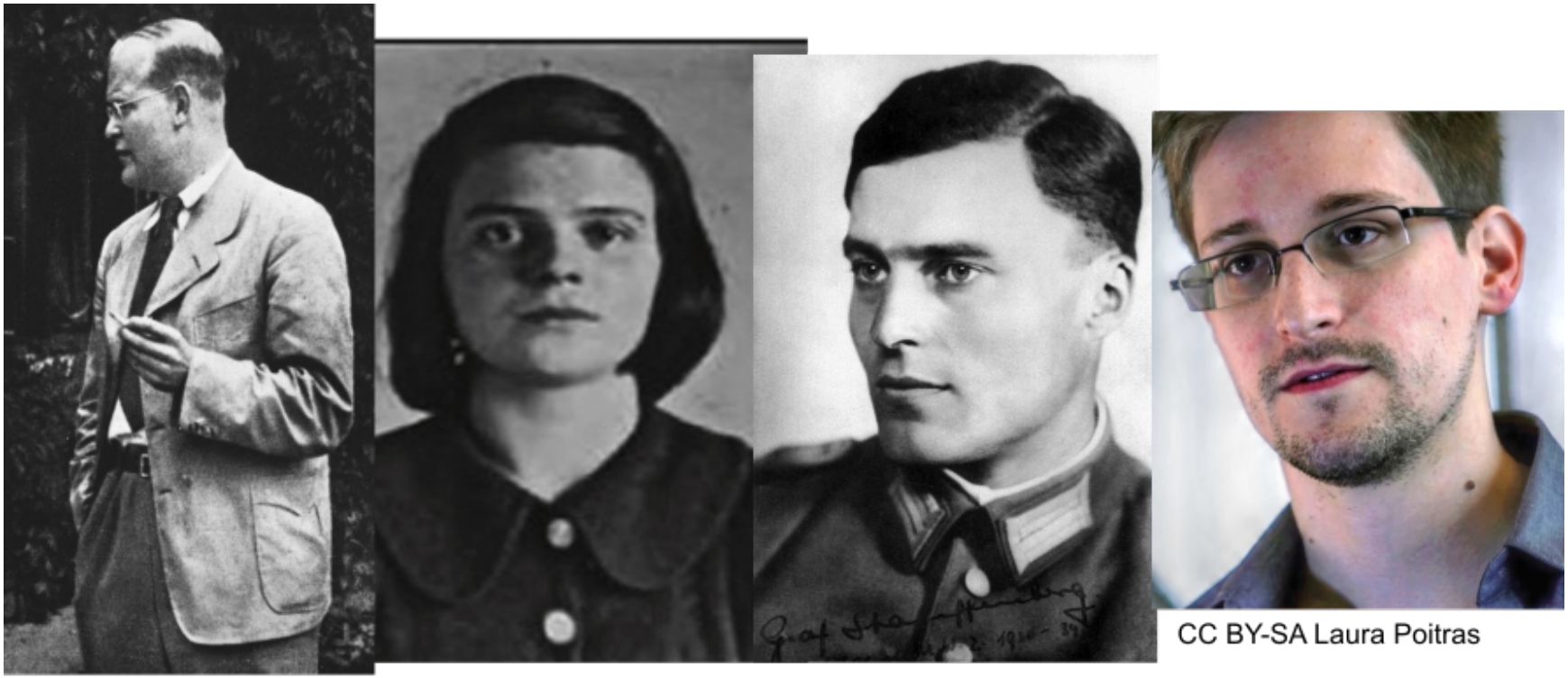
- amerikanische Server (also von Pratriot Act betroffen)
- spendenbasiert, kostenlos
- zwingend an Telefonnummer gebunden

Threema

- schweizer Firma, Server in der Schweiz
- kostet einmalig ca. 5 €
- muss nicht mit Telefonnummer verknüpft werden

Mein Tipp: Diese beiden Messenger installieren, mit dem Ziel irgendwann WhatsApp deinstallieren zu können.

Was mich manchmal traurig macht ...



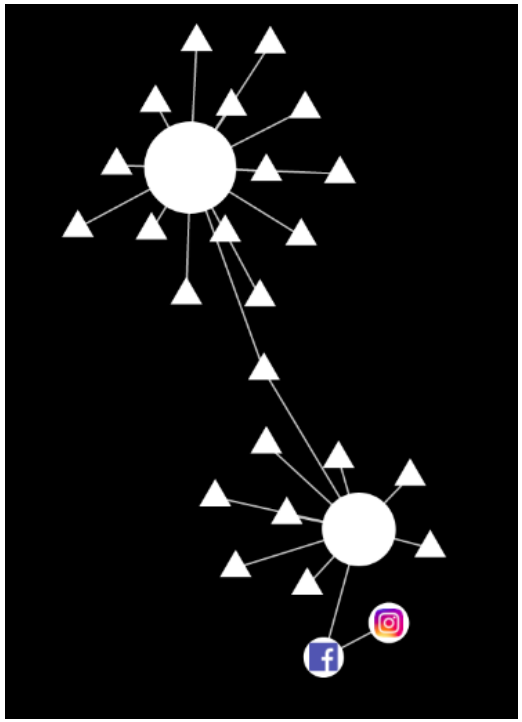
Bundesarchiv CC BY-SA

CC BY-SA Laura Poitras

Was hast du gerade gesagt? "Es sind doch nun mal alle bei WhatsApp und 5€ sind zu teuer?"

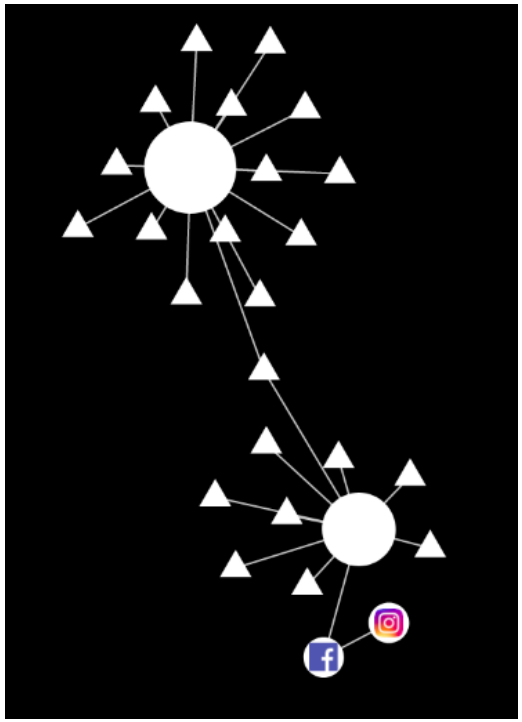
Tracking

- Nutzer wird über mehrere Domains hinweg verfolgt.
- Auf `amazon.de` nach Sneakern gesucht, auf `https://www.spiegel.com/` Werbung für Sneaker bekommen.
- demdex.net überwacht beide ...



Tracking beim Surfen

- Tracking selbst untersuchen mit Add-On Lightbeam
- `https://addons.mozilla.org/de/firefox/addon/lightbeam-3-0`



Konkrete Maßnahmen

- Add-On installieren, das das Nachladen von Dritt-Domains verhindert.
- Dies verhindert auch das Laden von Schad-Code
- Z.B. Privacy-Badger `https://privacybadger.org/`
- Oder UBlock Origin `https://addons.mozilla.org/de/firefox/addon/ublock-origin/`

Cookies - Werkzeug für Tracking

- Cookie = kleine Datei, die von Webseiten auf deinem Handy / Rechner abgelegt wird
- Dient dazu, dich wiederzuerkennen. (Du bist diejenige, die vorhin nach Adidas-Sneakern gesucht hat ...)
- Cookies ständig löschen -> Tracking ist sehr viel schwerer
- Cookies verbieten -> Manche Webseiten funktionieren nicht, z.B. Moodle

Konkrete Maßnahmen

- Add-On installieren, das Cookies löscht, sobald diese nicht mehr gebraucht werden.
- Empfohlen: Cookie AutoDelete
- `https://addons.mozilla.org/de/firefox/addon/cookie-autodelete`
- Muss nach Installation erst scharf geschaltet werden: Automatisches Aufräumen aktivieren

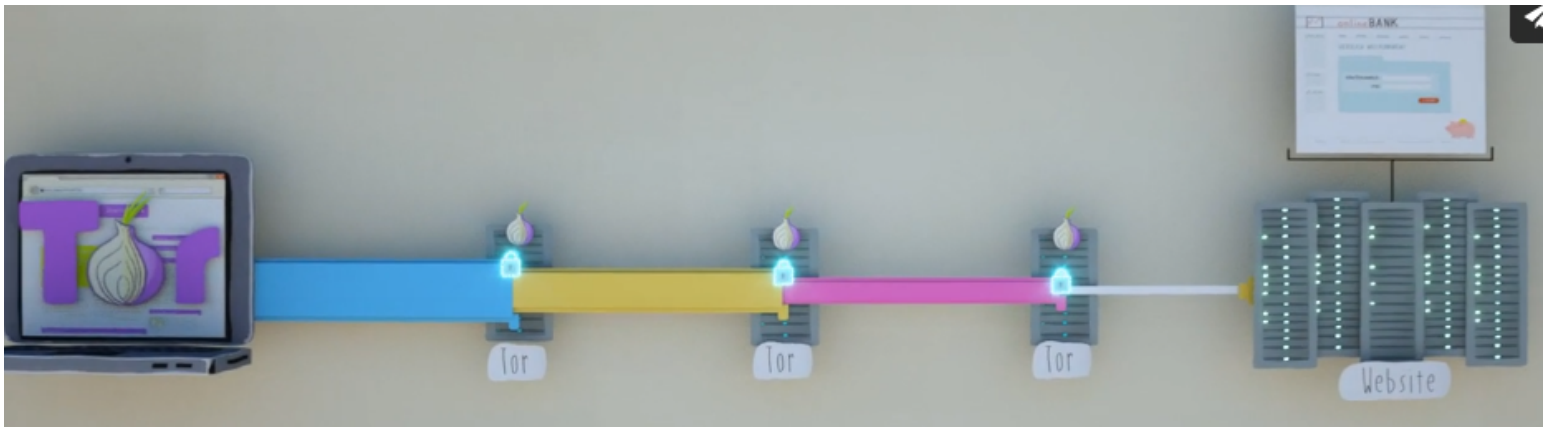
Datensparsames Surfen: Das 3-Browser-Konzept

1. TOR-Browser für alles außer Seiten, auf denen man sich einloggt. (Aus Ökogründen auch keine Videos, Downloads großer Dateien)
2. Browser, z.B. Firefox, mit
   - **Addons gegen Tracking**, z.B. uBlock Origin und
   - **Addons für das Löschen von Cookies**, z.B. Cookie Autodelete
3. Browser ohne Trackingschutz für Seiten, für die der Browser 2 nicht funktioniert

Erklärung des 3-Browser-Konzepts

`https://www.kuketz-blog.de/das-3-browser-konzept-not-my-data-teil2/`

Was ist TOR



- Anonymisierungsnetzwerk
- Selbst der Webseitenbetreiber weiß nicht, von welcher IP-Adresse man kommt
- Pakete werden mehrfach verschlüsselt und nehmen zur Verschleierung einen längeren Weg durchs Internet
- Super Erklärvideo: `https://vimeo.com/164049726`

Privates Fenster

Achtung: Beliebter Denkfehler!

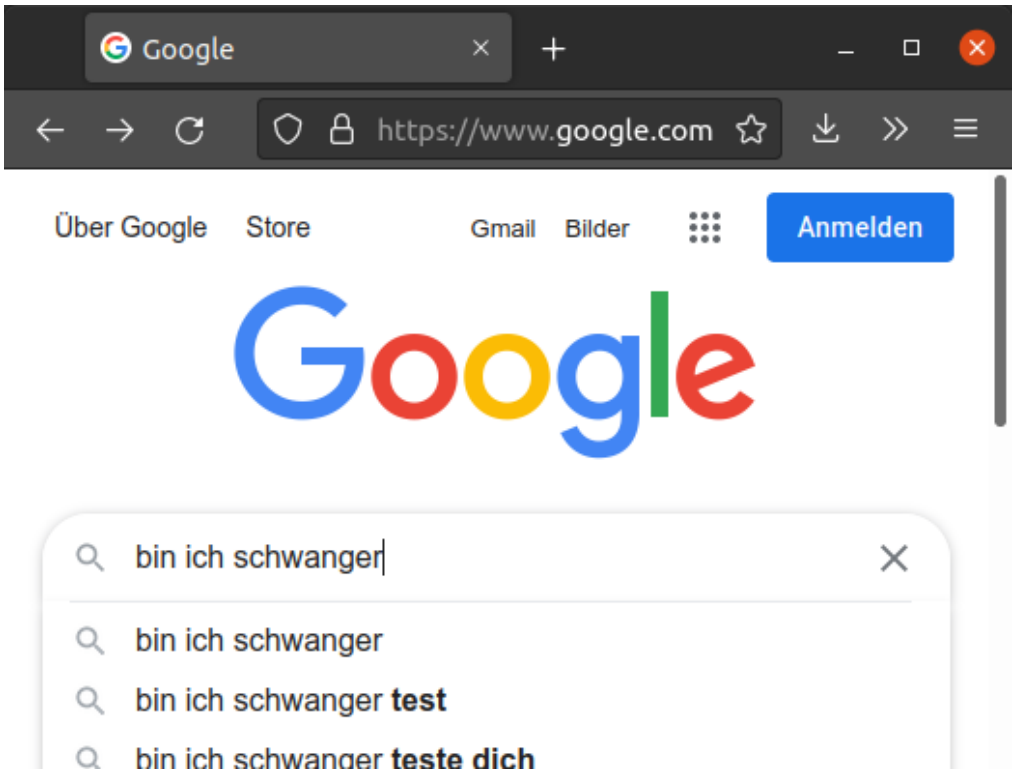
Privates Fenster

- Bietet **keine** Anonymität gegenüber Anbietern!
- Hinterlässt aber keine Spuren auf dem lokalen Rechner / Handy
- Auch „Pornomodus“genannt. Warum?

Auswahl von Diensten: Mail-Provider

- Welches Geschäftsmodell? Zahlen mit Daten oder Zahlen mit kleinem Eurobetrag?
- Z.B. bei gmail (von Google) akzeptiert man das automatisierte Scannen der Mails (z.B. für personalisierte Werbung)
- Gute Alternativen:
  - Posteo (1€ pro Monat)
  - Mailbox.org (1€ pro Monat)
  - Tutanota (auch kostenlos möglich, einfache Verschlüsselung ohne PGP)

Auswahl von Diensten: Suchmaschine



Jede Frage an eine Suchmaschine ist eine Antwort.

- unbedingt Standardsuchmaschine im Browser ändern.
- Google ist voreingestellt und somit fließen Daten an einen ohnehin schon zu mächtigen Player.

Suchmaschinen - Eine Machtfrage

- Nutzen alle die gleiche Suchmaschine, kann deren Betreiber festlegen, was gefunden wird!
- Unternehmen, die nicht hoch gerankt sind, sind tot!
- Mangelnde Transparenz: PageRank-Algorithmus von Google nicht bekannt!
- Bei Suchmaschinen-Monopol Zensur möglich

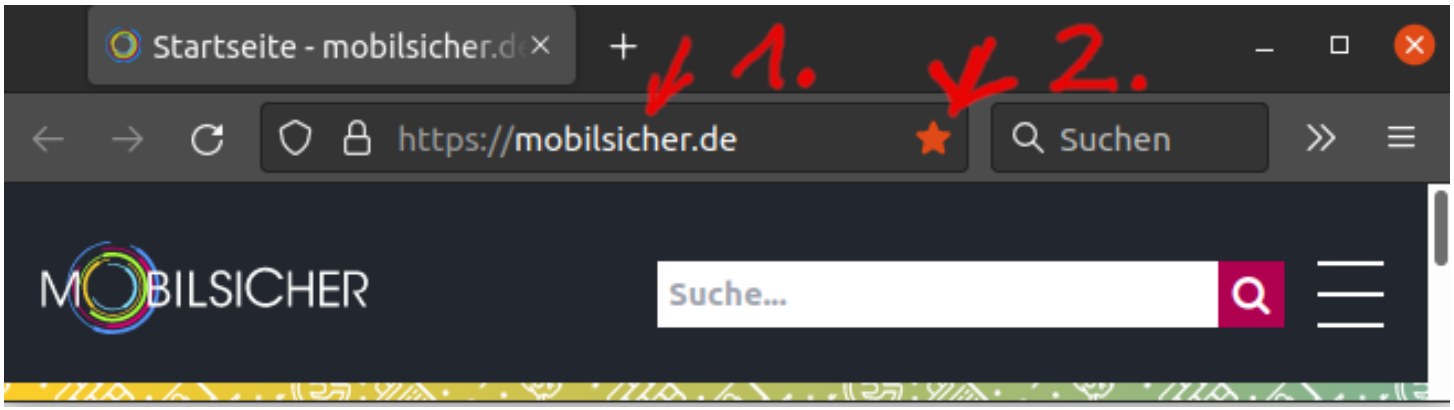
Empfehlenswerte Suchmaschinen

- Duckduckgo (amerikanisch)
  `https://duckduckgo.com/`
- Metager (deutsch) `https://metager.de/`
- Ecosia (öko) `https://www.ecosia.org`
- Startpage (anonymisierte Google-Ergebnisse)
  `https://www.startpage.com/`
- Qwant (französisch) `https://www.qwant.com/`

`https://mobilsicher.de/ratgeber/suchmaschinen-die-fuenf-besten-alternativen-zu-google`

Zusätzlich bei Suchmaschinen zu beachten:

1. Bekannte Adressen immer in die Adressleiste (ganz oben im Browser) eingeben, nicht in ein Suchfeld – das spart auch Strom
2. Lesezeichen setzen für Seiten, die man öfter benutzt



Auswahl von Diensten: Der Kartendienst Openstreetmaps

- durch Nutzung von Google Maps landen weiter aussagekräftige Daten bei einem großen Player
- gute Alternative ist **Openstreetmaps**
- im Browser `https://www.openstreetmap.org`
- mobile App OsmAnd+ (Openstreetmaps and More)
- Karten lokal speicherbar, **Navigation ohne Netzempfang möglich!**

Auswahl von Diensten: Alternativen suchen

- Dienste, die eine Einwilligung erpressen, meiden!
- nach Alternativen suchen

Apps auf dem Handy

- Apps immer nur die Berechtigungen erteilen, von denen plausibel ist, dass sie gebraucht werden.
- z.B. braucht eine App für Textbearbeitung sicher keinen Standort
- Nur Apps auf dem Handy haben, die man **wirklich aktuell benötigt**.
- Also immer wieder aufräumen und **nicht mehr benötigte Apps löschen**.
- Vor dem Löschen überlegen: Gibt es einen **Account** beim Anbieter, den man erst noch **löschen** muss?
  Sonst bleiben Daten beim Anbieter.

Apps auf dem Handy – F-Droid

- Empfehlung: Möglichst nur Apps aus dem **F- Droid-Store** nutzen
- Dann ist später ein Wechsel auf google-freies Android möglich.
- Apps im F-Droid-Store sind trackingfrei.

Apps auf dem Handy – Tracker-frei?

- Datenbank mit vielen Apps und deren Tracker
- `https://appcheck.mobilsicher.de/`

Proprietäre Software versus FOSS

Proprietär:

- Windows, Microsoft Office, alles von Apple ...
- Lock-In-Effekt: NutzerIn investiert Zeit, um sich mit der Bedienung vertraut zu machen. Wird alle Änderungen an den Rahmenbedingungen akzeptieren.
- NutzerIn ist abhängig vom Hersteller
- Produkte senden oft Nutzerdaten an den Hersteller

Proprietäre Software versus FOSS

Free and Open Source Software

- Linux, Libre Office, Open Office, Firefox, Thunderbird
- Man muss keine AGB lesen und akzeptieren
- kein Lock-In-Effekt
- Selbst wenn es Änderungen gibt, die man nicht gut findet, kann man auf Forks hoffen: Freiwillige pflegen Versionen der Software in ihrer Freizeit weiter
- Senden von Nutzerdaten kann man in der Regel abwählen

Die datenbewusste BürgerIn nutzt Linux

Den Umstieg vorbereiten:

- zunächst beim gewohnten Betriebssystem bleiben (z.B. Windows), dort aber immer weiter an Software gewöhnen, die es auch für Linux gibt
- Libre oder Open Office statt MS Word
- Firefox statt Edge
- Thunderbird statt Outlook
- Wenn diese Umgewöhnung geglückt ist, ist der Umstieg auf Linux keine große Hürde mehr.

Dringende Empfehlung: Passwortmanager

- Passwörter sollten mind. 14 Zeichen lang sein und komplex
- **KEINE Mehrfachverwendung!**
- Lösung: Passwortmanager, z.B. KeepassXC
- Ganze Passwortsammlung wird mit einem sehr langen, sehr sicheren Master-Passwort geschützt
- ABER Achtung: Masterpasswort muss SEHR STARK gewählt werden.

Auswahl der Apps und Programme

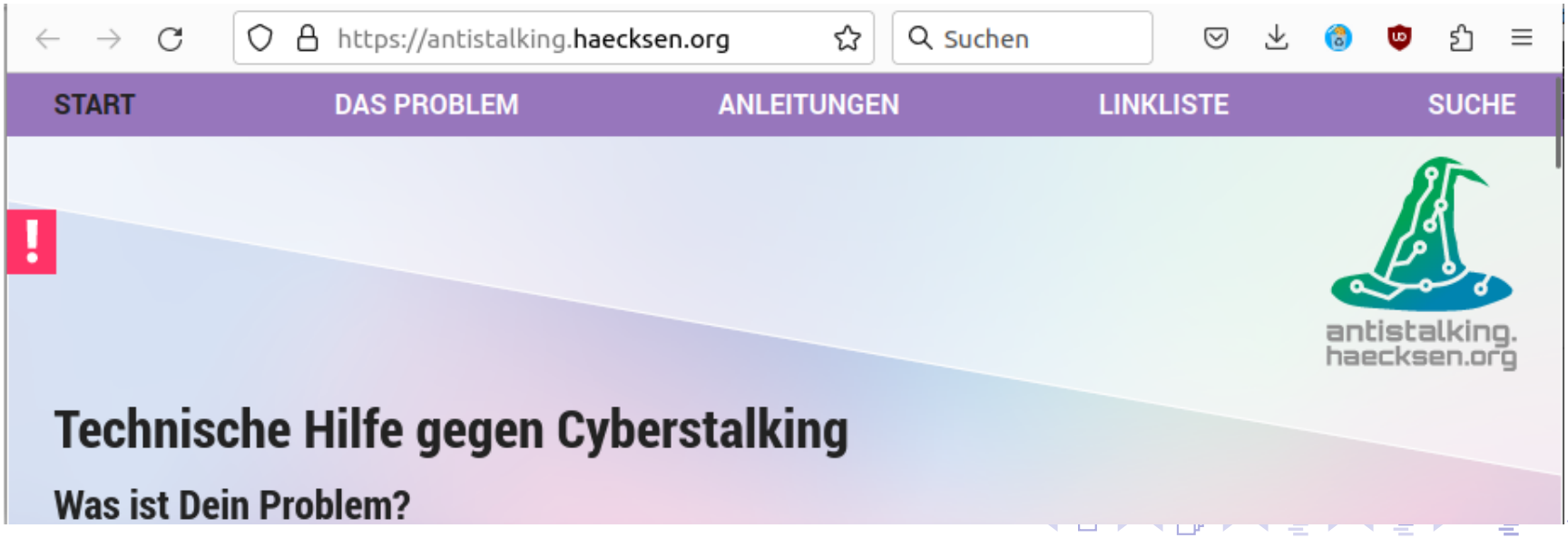
https://www.cryptoparty.in/learn/tools

Stalking

- Oft richtet der Mann die Geräte seiner Partner*In ein, weil diese sich das nicht zutraut.
- Der Mann hat dadurch sämtliche Zugangsdaten.
- Kann im Fall einer Trennung zum Problem werden.

Stalking

- Besser vorbeugen: Alle Geräte und Konten selbst einrichten. Die Zugangsdaten NICHT dem Partner geben.
- Hilfe für Betroffene:
  `https://antistalking.haecksen.org`



Gute Informationsquellen

- Anfängerinformationen für Handynutzer, auch Videos:
  `https://mobilsicher.de/`
- super Erklärvideos von Alexander Lehmann
  `https://vimeo.com/alexanderlehmann`
- Die Organisation mit dem Negativpreis, auch Anleitungen:
  `https://digitalcourage.de/`
- Eher für Fortgeschrittene:
  `https://www.kuketz-blog.de/`
- Interaktive Doku von Arte:
  `https://donottrack-doc.com`
- Konkrete Softwareempfehlungen
  `https://www.cryptoparty.in/learn/tools`

Danke für die Aufmerksamkeit!

- Download der Folien:
  `https://raw.githubusercontent.com/sylvialange/vortraege/main/beginner.pdf`
- Anregungen für Hands-On-Teil:
  `https://raw.githubusercontent.com/sylvialange/vortraege/main/handson.pdf`