# CryptoSeminar Bielefeld

## Digitale Selbstverteidigung gegen Massenüberwachung

digitalcourage Hochschulgruppe

(Bild: CC-BY, Daniela Vladimirova)

# Kurze Vorstellung

- Georg Gottleuber
- Sebastian Lisken
- Leif Rottmann
- Jan Schötteldreier

# 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
  - CryptoPartys
  - Backup-Partys
  - Linux-Install-Partys
  - Regelmäßige Treffen an der Uni

# CryptoParty

- Digitale Selbstverteidigung
- Schutz vor Massenüberwachung

- Öffentlich, nicht-kommerziell, weltweit


- 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 Freitag

| von | bis | Titel |
|---|---|---|
| 10:00 | 12:00 | Vortrag: Privatsphäre im Zeitalter der Massenüberwachung |
| 12:00 | 12:10 | - Kurze Pause - |
| 12:10 | 13:10 | Digitale Selbstverteidigung I<br>(W10, Passwörter) |
| 13:10 | 14:00 | - Mittagspause - |
| 14:00 | 15:30 | Digitale Selbstverteidigung II<br>(Datenträgerverschlüsselung, Browser) |
| 15:30 | 15:40 | - Kurze Pause - |
| 15:40 | 17:00 | Praxis |
| | | Open End |

https://digitalcourage.de/hsg

# Agenda Samstag

| von | bis | Titel |
|---|---|---|
| 10:00 | 11:00 | Digitale Selbstverteidigung III (E-Mails) |
| 11:00 | 11:15 | - Kurze Pause - |
| 11:15 | 13:00 | Praxis |
| 13:00 | 14:00 | - Mittagspause - |
| 14:00 | 15:00 | Digitale Selbstverteidigung IV (Mobilgeräte) |
| 15:00 | 15:15 | - Kurze Pause - |
| 15:15 | 17:00 | Praxis |
| | | Feedback, Diskussion / Open End |

# Privatsphäre im Zeitalter der Massenüberwachung – Eine Einführung in den Datenschutz

# Zwei einführende Beispiele

Neue technische Möglichkeiten

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

# Zwei einführende Beispiele

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

- AZ Direkt

# 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 ...

# 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

# Digitale Identität

# Google-Dienste

- Was für Dienste bietet Google an?

# Google Suchmaschine

- Marktanteil weltweit ca. 90%
- Als Standard vorinstalliert
  - Chrome, Firefox
  - Android (Widget, Gboard Tastatur)
- 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

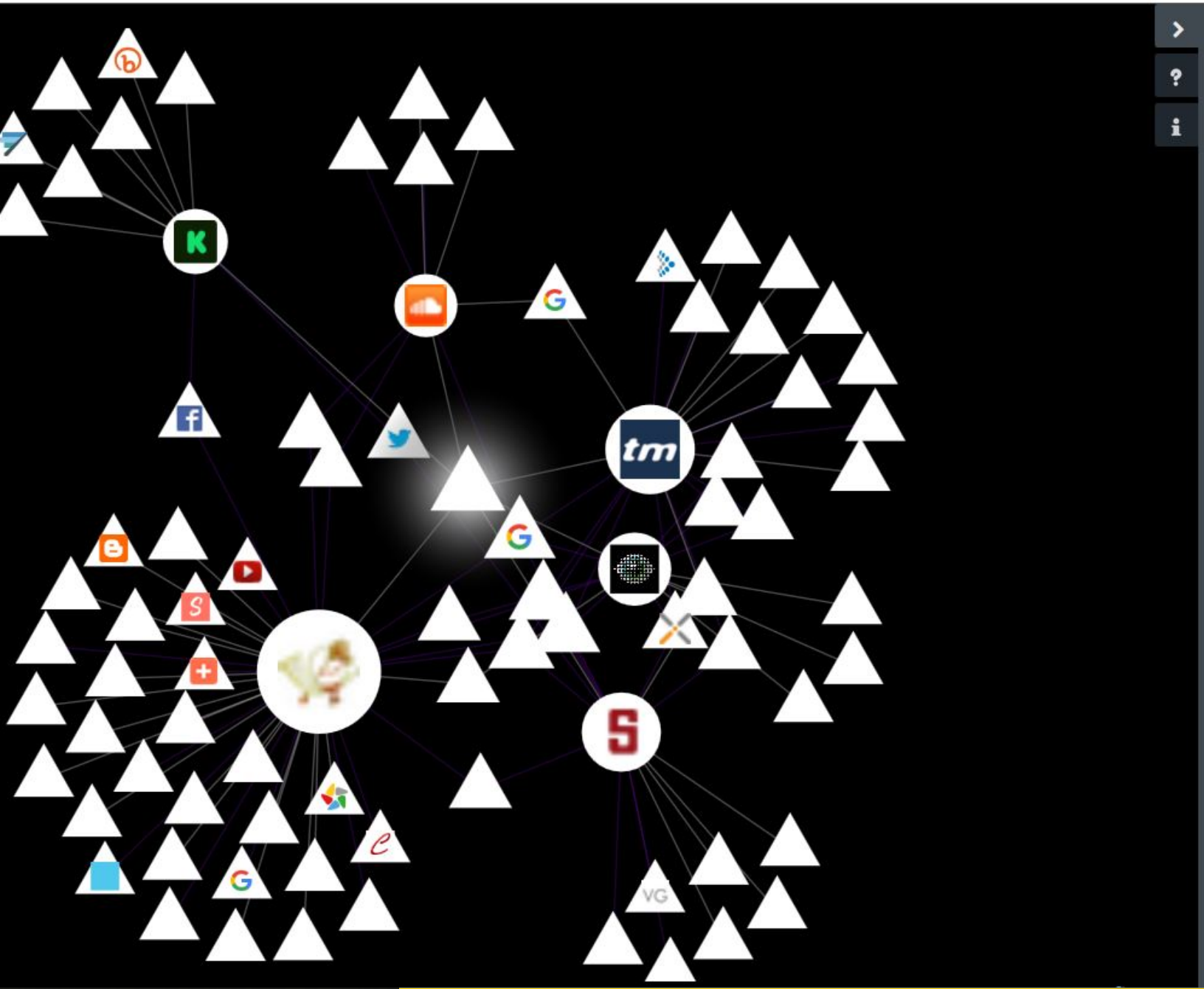
# Google Analytics

- 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)

# Event Tracking

- Tracking der Interaktion mit der Webseite
  - Klick auf interne Links (Navigation, Teaser)
  - Klick auf externe Links
  - Interaktion mit Videos (zu wieviel % abgespielt)
  - Scrollverhalten
  - ...

TRACKING PROTECTION OFF



google-analytics.com

**FIRST ACCESS** Tue, May 23, 2017 7:52AM
**LAST ACCESS** Tue, May 23, 2017 7:52AM

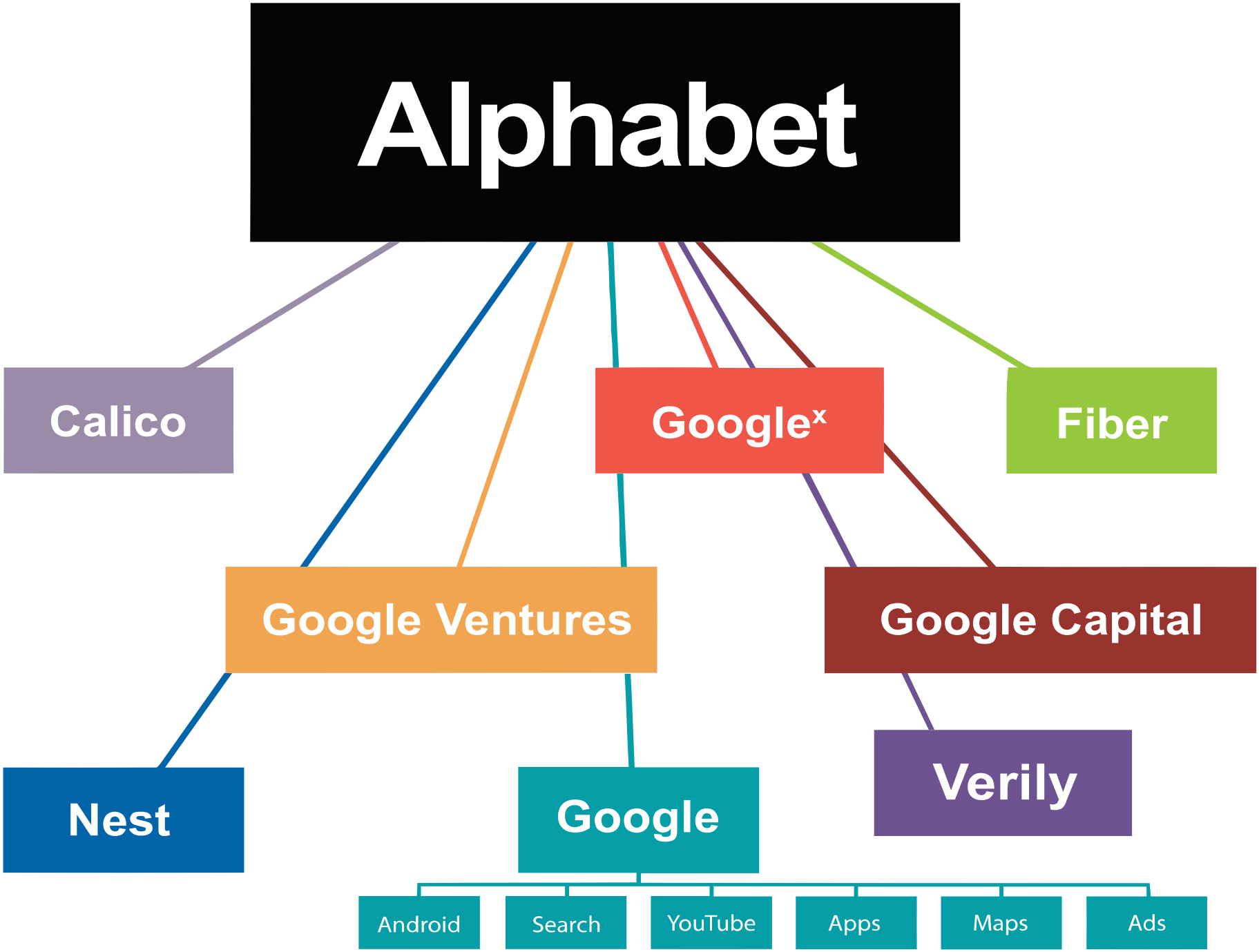
Block Site

## Server Location

United States

Connected to **6 sites** since first access.

spiegel.de
soundcloud.com
kickstarter.com
transfermarkt.de
golem.de
der-postillon.com


Alphabet
Calico
Google[x]
Fiber
Google Ventures
Google Capital
Nest
Google
Verily
Android
Search
YouTube
Apps
Maps
Ads

# 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)

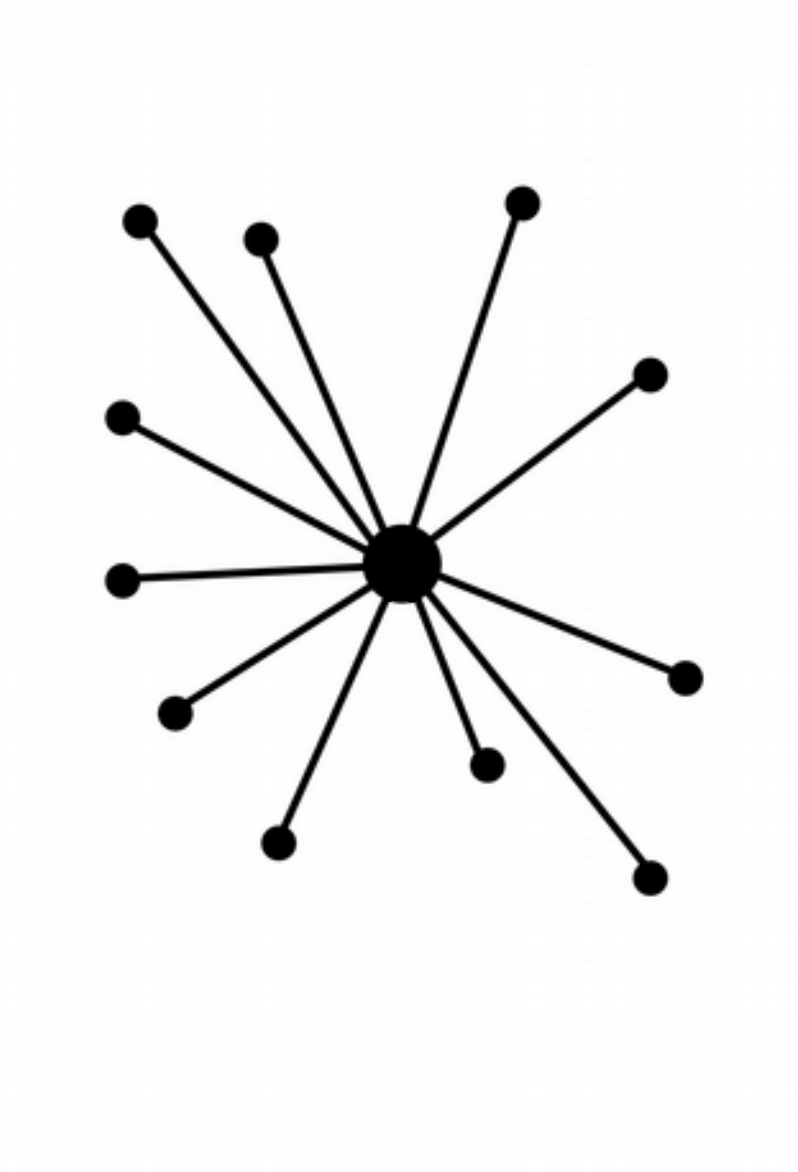
# Datenwirtschaft

- "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

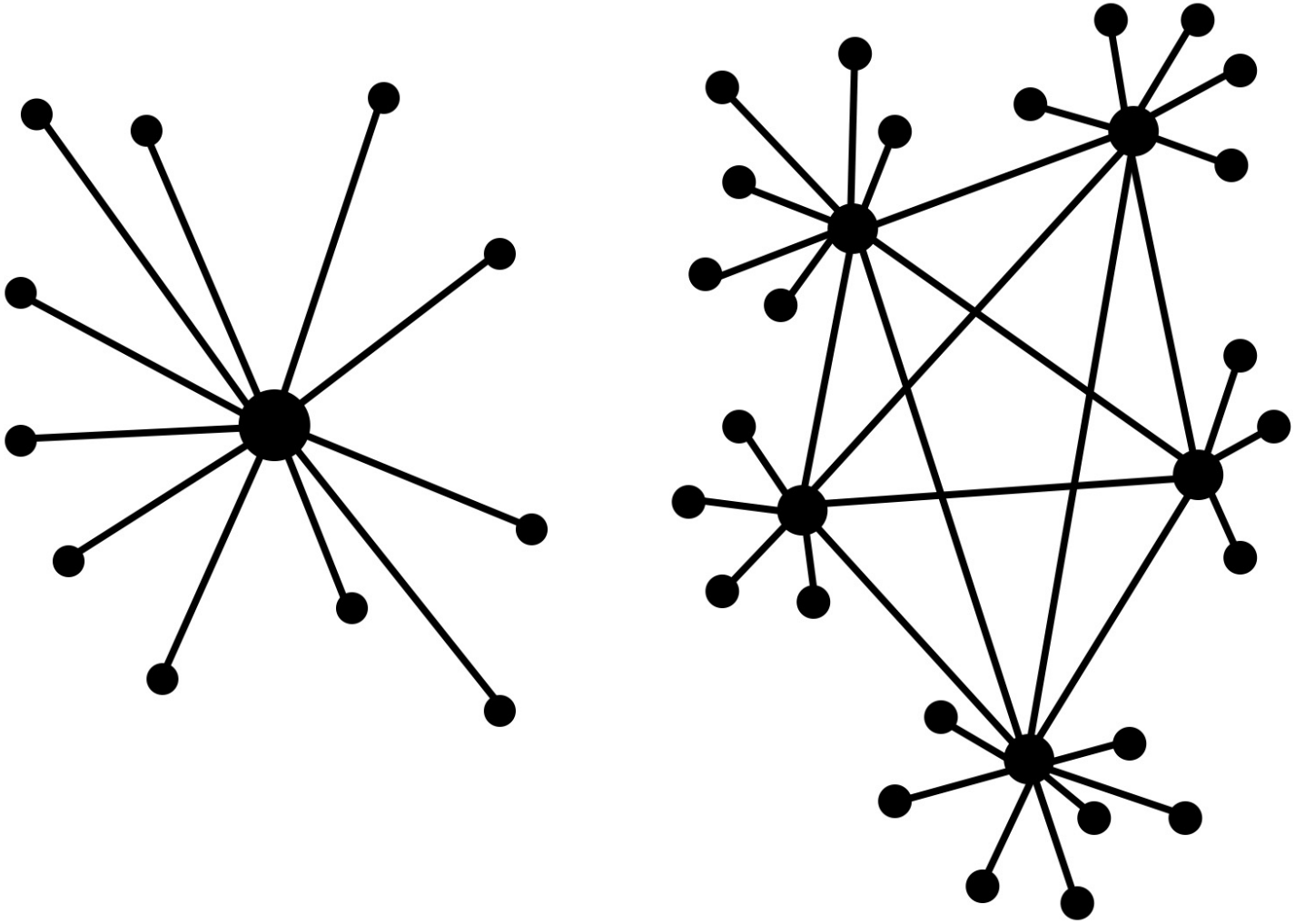
# Datenwirtschaft

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

# 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

# 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 verfassungswiedrig 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.

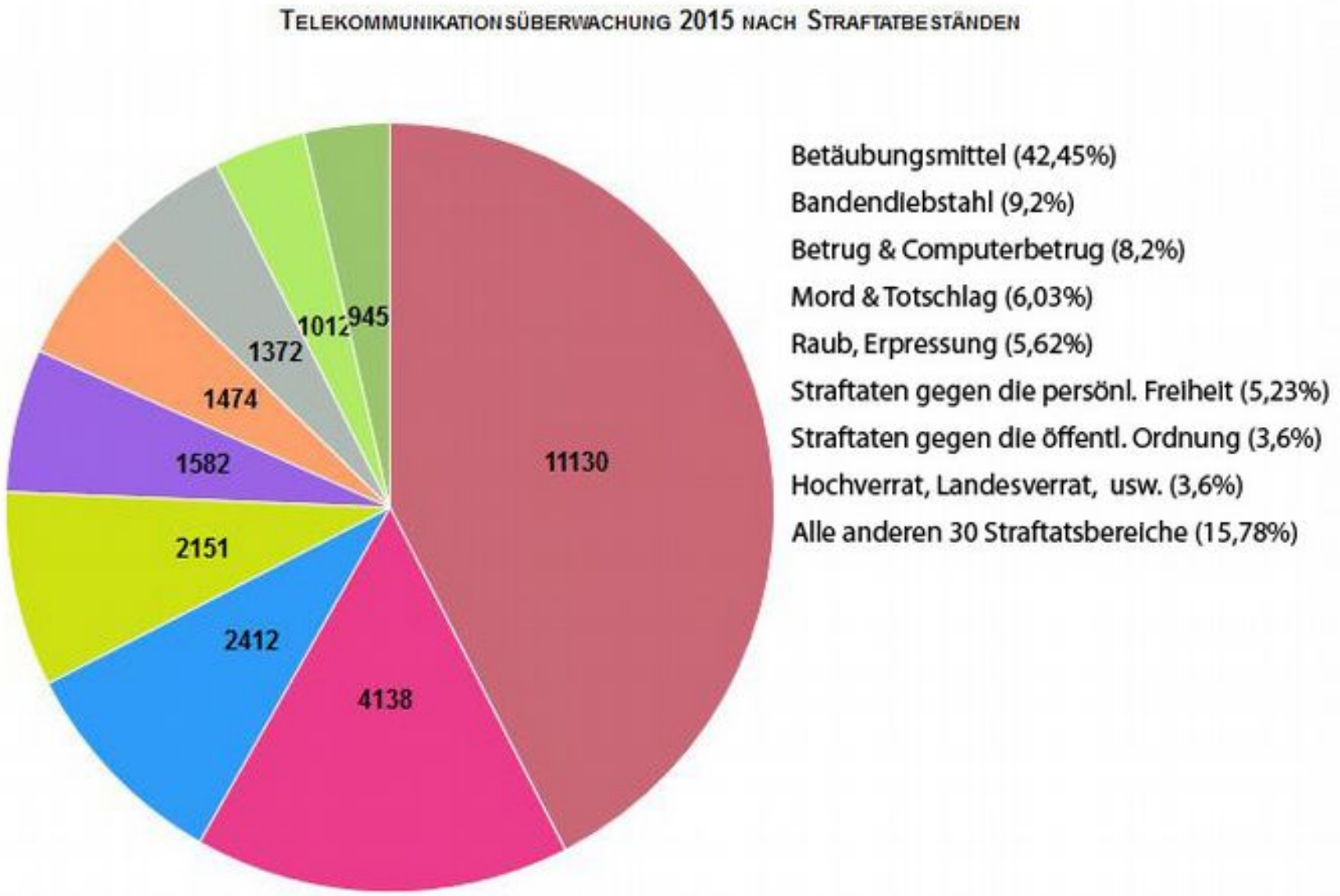
# VDS: Was wird gespeichert?

- 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://apps.opendatacity.de/vds/

- Malte Spitz (Grüne, Deutschland):
  http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten




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

# Freie Entfaltung der Persönlichkeit

Grundgesetz, Artikel 2

# Auswahl von Überwachungsgesetzen und -maßnahmen 2016

| Geheimdienste und Behörden | Gesetze und Gesetzesentwürfe | Politische Forderungen | Privatwirtschaft & Überwachung | Gesetze und -entwürfe Europa | Datenbanken Europa | Gesetze im Ausland |
|---|---|---|---|---|---|---|
| Zitis | Anti-Terror-Gesetz (u.a. Ausweise für SIM) | Ausweitung VDS auf Messenger | Uploadfilter in sozialen Netzwerken | PNR Fluggast-daten | Fluggast-daten PNRDEP | Snoopers Charter UK |
| ANISKI | BND-Gesetz | Aufweichung Provider-privileg | Yahoo durchsuchte alle E-Mails | Schutz von Geschäfts-geheim-nissen | ADEP | Anti-Terror-Gesetz in Polen |
| Bund: Höhere Budgets Geheim-dienste | Datenaus-tauschs-verbesserungs gesetz | Gesichts-erkennung bei Video-überwachung | Ausweitung der Video-überwachung | Mehr Europol-Befugnisse + Meldestelle Internet | Reiseregister EET & ETIAS | Ausnahme-zustand in Frankreich |
| Bayerischer VS: Zugriff auf Vorratsdaten | Videoüberwac hungsver besserungs-gesetz | Verbot von Fake News | US-Wahlkampf: Targeting mit Psychometrie | Eröffnung Europäisches Anti-Terror-Zentrum Dem Haag | Erweiterung Eurodac | Geheimdienst-Gesetz in Niederlande |
| Mobiler Staats-trojaner | Novelle BDSG | Verlängerung Speicherfrist VDS | Facebook speichert ethnische Zugehörigkeit | EU-Anti-Terror-Richtlinie | Zusammen-legung der „Datentöpfe“ | Staatsschutz-gesetz in Österreich |

# Neu von 2017

- Bodycams und Kennzeichen-Scanner für die Bundespolizei
- Gesetz zur besseren Durchsetzung der Ausreisepflicht
- Fluggastdatengesetz (PNR-Weitergabe)
- Gesetz zur Förderung des elektronischen Identitätsnachweises
- Ausweitung der Vorratsdatenspeicherung
- Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens

Quelle: https://netzpolitik.org/2017/chronik-des-ueberwachungsstaates/

# Bundesdatenschutzgesetz

- Datensparsamkeit
  - So wenig personenbezogene Daten wie möglich erheben
- Zweckbindung
  - Personenbezogene Daten nur für vorher festgelegte und rechtmäßige Zwecke verwenden
- Informationelle Selbstbestimmung
  - Selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten bestimmen

Ab 25.05. wird in der ganzen EU die Datenschutz-Grundverordnung (DSGVO) anwendbar.

# 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/

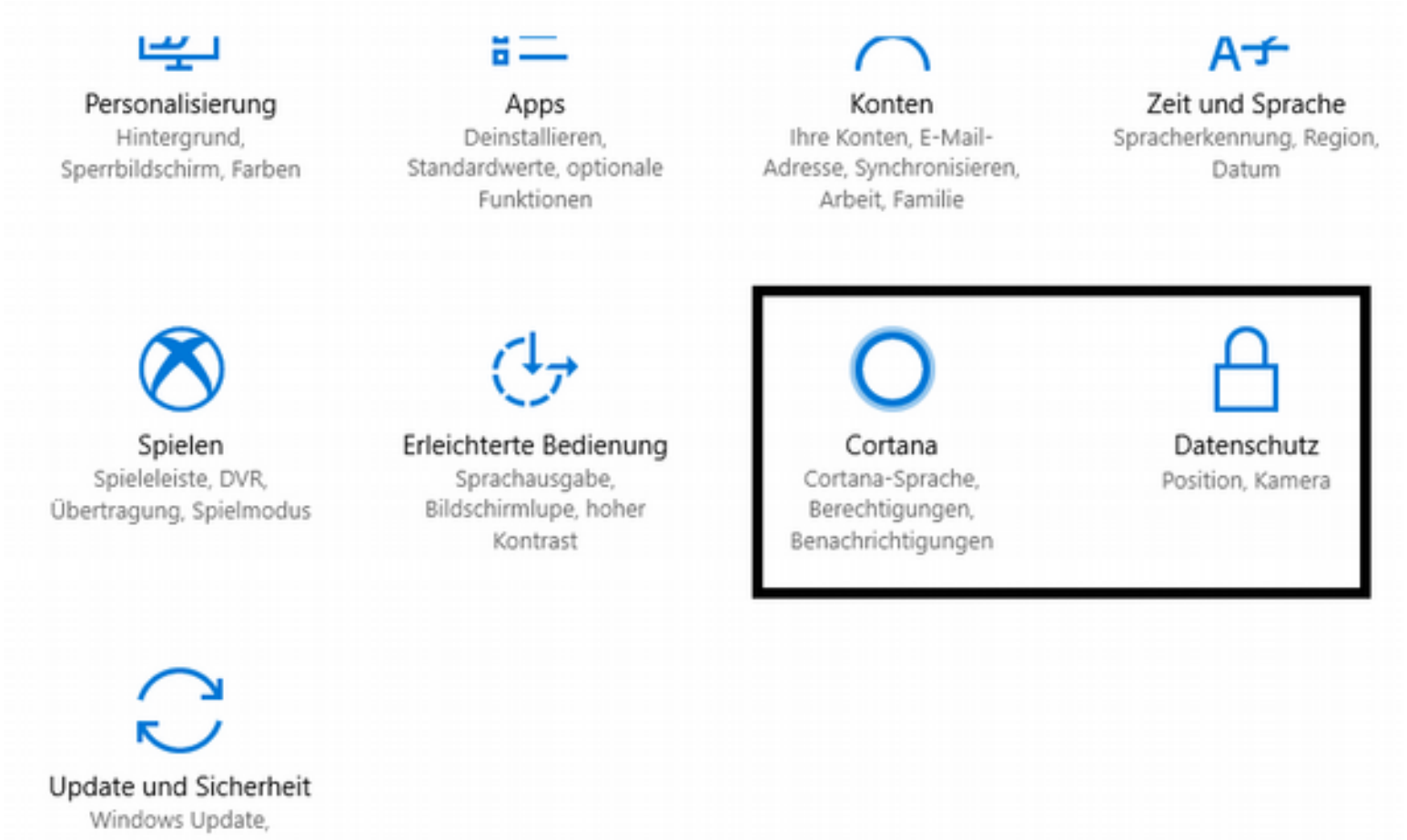
- Kurze Pause -

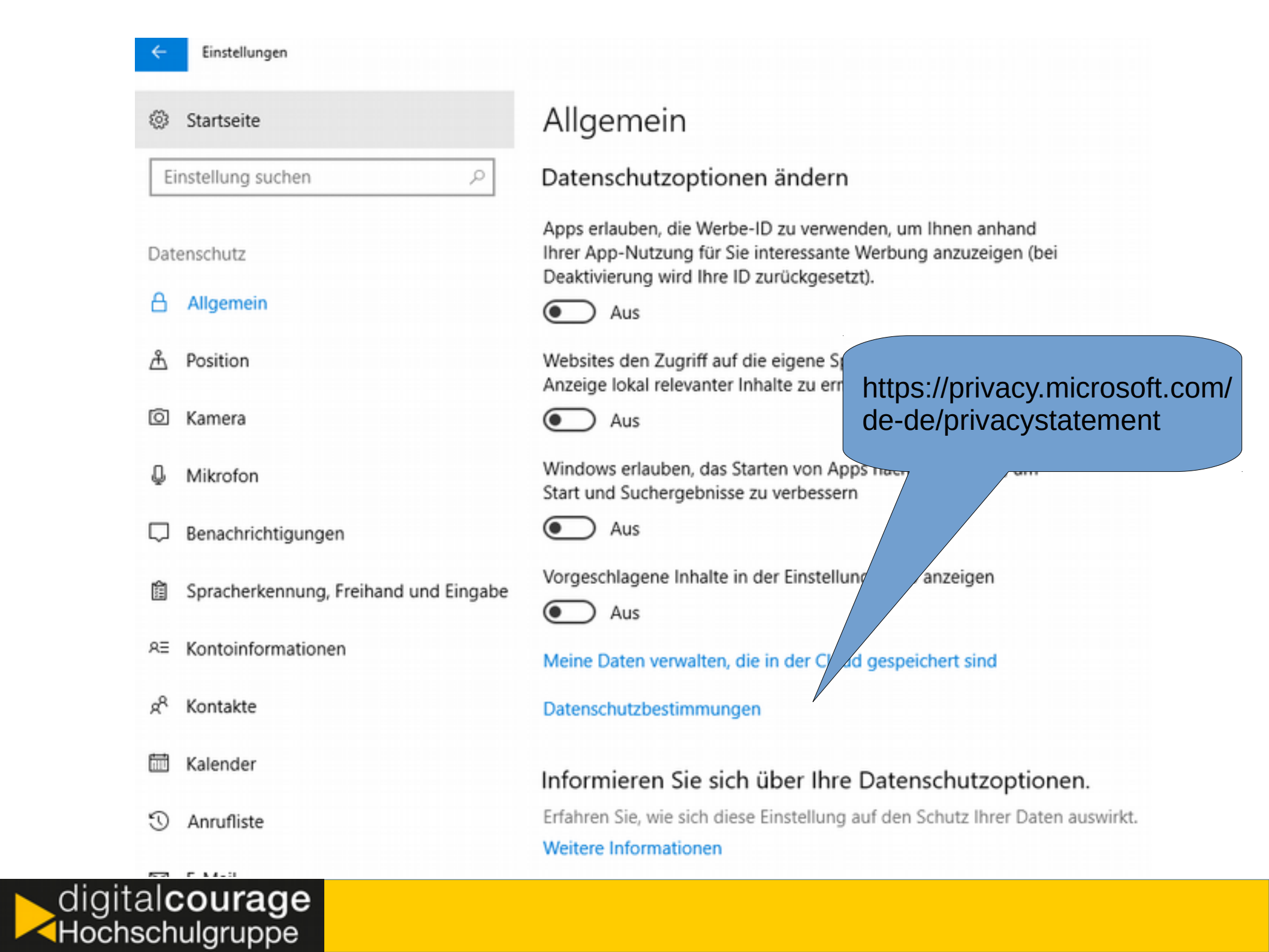
# "Datenschutzalbtraum" Windows 10

# "Datenschutzalbtraum" Windows 10?

- Windows Store mit zahlreichen vorinstallieren Apps
  - z.B. Cloud-Dienst "OneDrive" oder Browser und PDF-Reader "Edge"
- "Sprachassistentin" Cortana
  - Automatische Installation
  - Nur schwer aus dem System zu löschen
- Systemupgrades, die nur aufgeschoben werden können
  - aktuell "April 2018 Update" Windows 10 Version 1803, Build 17134, Codename Redstone 4

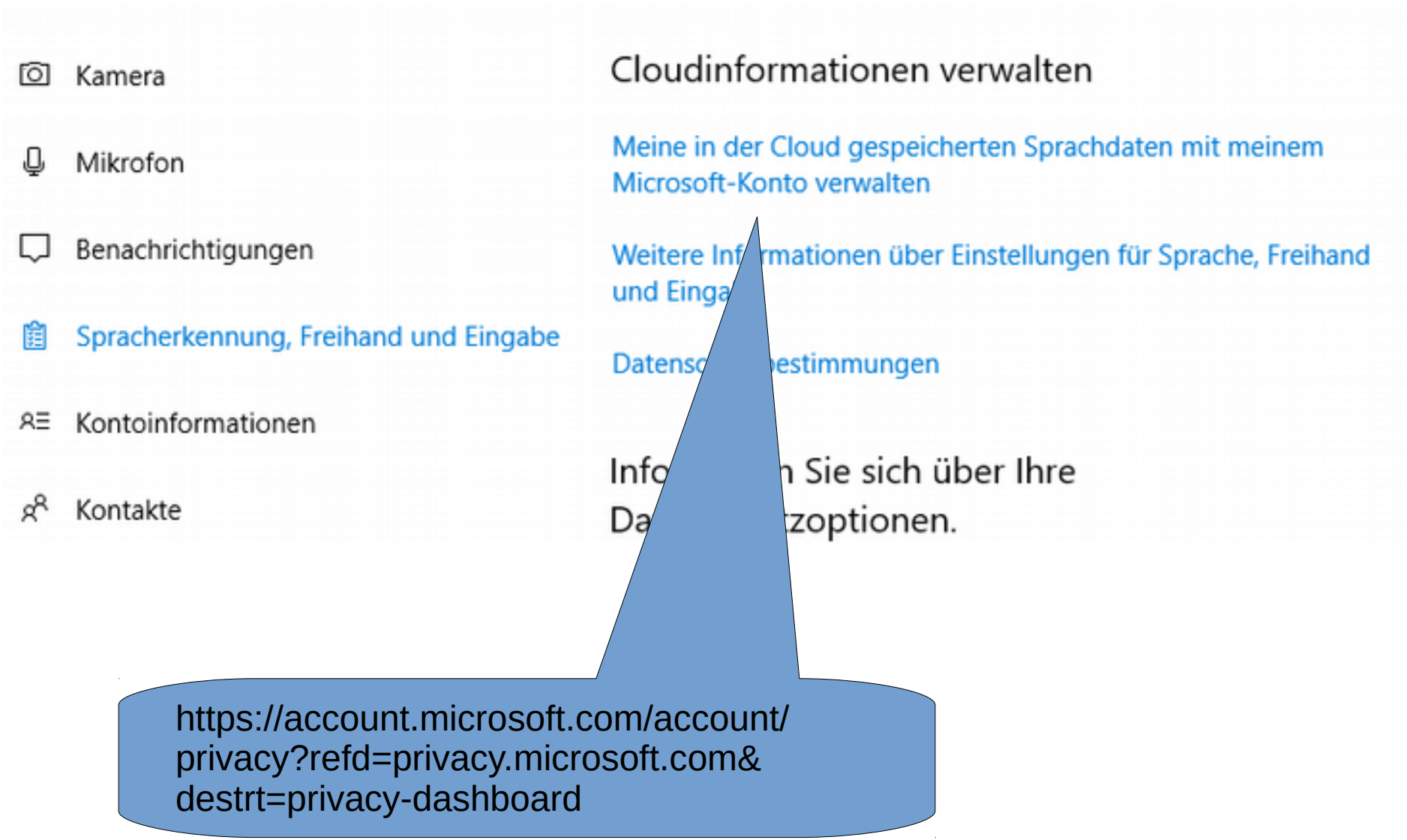
# Wichtige Einstellungen



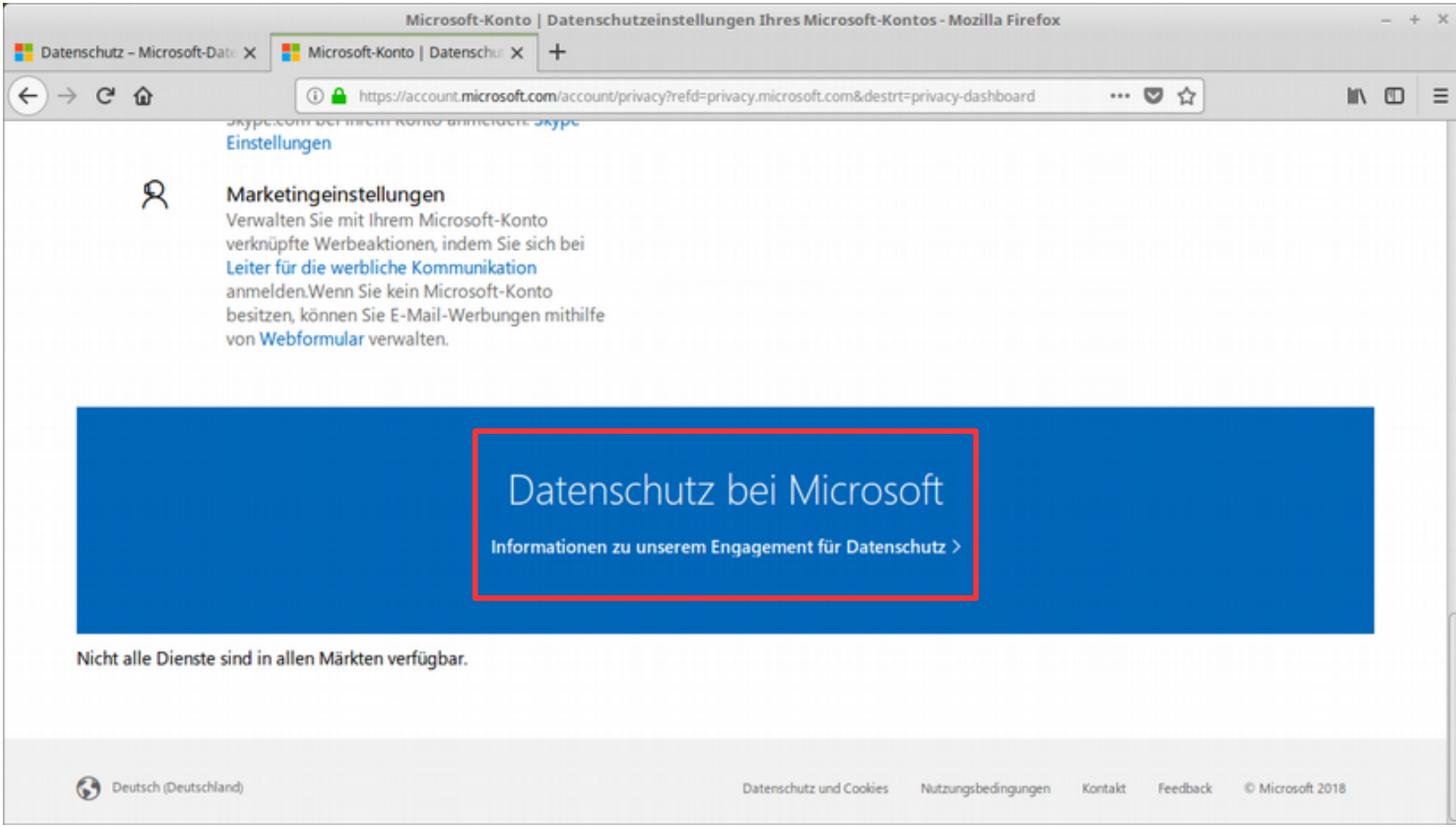

Einstellungen
Startseite
Einstellung suchen
Datenschutz
Allgemein
Position
Kamera
Mikrofon
Benachrichtigungen
Spracherkennung, Freihand und Eingabe
Kontoinformationen
Kontakte
Kalender
Anrufliste
Allgemein
Datenschutzoptionen ändern
Apps erlauben, die Werbe-ID zu verwenden, um Ihnen anhand Ihrer App-Nutzung für Sie interessante Werbung anzuzeigen (bei Deaktivierung wird Ihre ID zurückgesetzt).
Aus
Websites den Zugriff auf die eigene Sp
Anzeige lokal relevanter Inhalte zu err
Aus
Windows erlauben, das Starten von Apps
Start und Suchergebnisse zu verbessern
Aus
Vorgeschlagene Inhalte in der Einstellun
anzeigen
Aus
Meine Daten verwalten, die in der Cl
d gespeichert sind
Datenschutzbestimmungen
https://privacy.microsoft.com/de-de/privacystatement
Informieren Sie sich über Ihre Datenschutzoptionen.
Erfahren Sie, wie sich diese Einstellung auf den Schutz Ihrer Daten auswirkt.
Weitere Informationen

# Datenschutzerklärung

- "Microsoft erhebt Daten, um effektiv arbeiten und Ihnen die besten Erfahrungen mit unseren Produkten anbieten zu können. Sie stellen einige dieser Daten direkt bereit, beispielsweise wenn Sie ein Microsoft-Konto erstellen, eine Suchanfrage bei Bing einreichen, einen Sprachbefehl an Cortana erteilen, [... können wir] Ihre Interaktion mit unseren Produkten aufzeichnen [...] Wir erhalten ebenfalls Daten von Drittanbietern."
  https://privacy.microsoft.com/de-de/privacystatement
- Zweck der Sammelwut: mit den Daten der eigenen Kunden Geld verdienen!


Kamera
Mikrofon
Benachrichtigungen
Spracherkennung, Freihand und Eingabe
Kontoinformationen
Kontakte
Cloudinformationen verwalten
Meine in der Cloud gespeicherten Sprachdaten mit meinem Microsoft-Konto verwalten
Weitere Inf rmationen über Einstellungen für Sprache, Freihand und Einga
Datensc estimmungen
Info n Sie sich über Ihre
Da zoptionen.
https://account.microsoft.com/account/privacy?refd=privacy.microsoft.com&destrt=privacy-dashboard

# Daten in der Cloud



"Hallo, ich bin Satya Nadella
und CEO von Microsoft.
Hier sind meine Versprechen

Wir bei Microsoft möchten alle Benutzer und Unternehmen dabei unterstützen, mehr zu erreichen. Wir entwickeln eine intelligente Cloud, neue Bürosoftware sowie Geschäftsprozesse und gestalten die Computerarbeit persönlicher. Bei all dem setzen wir selbstverständlich wie schon immer auf Datenschutz. Sie behalten die Kontrolle über Ihre Daten.

Sie entscheiden, wie und warum Daten erfasst und genutzt werden. Außerdem stellen wir sicher, dass Sie stets informierte Entscheidungen zu unseren Produkten und Diensten treffen können.

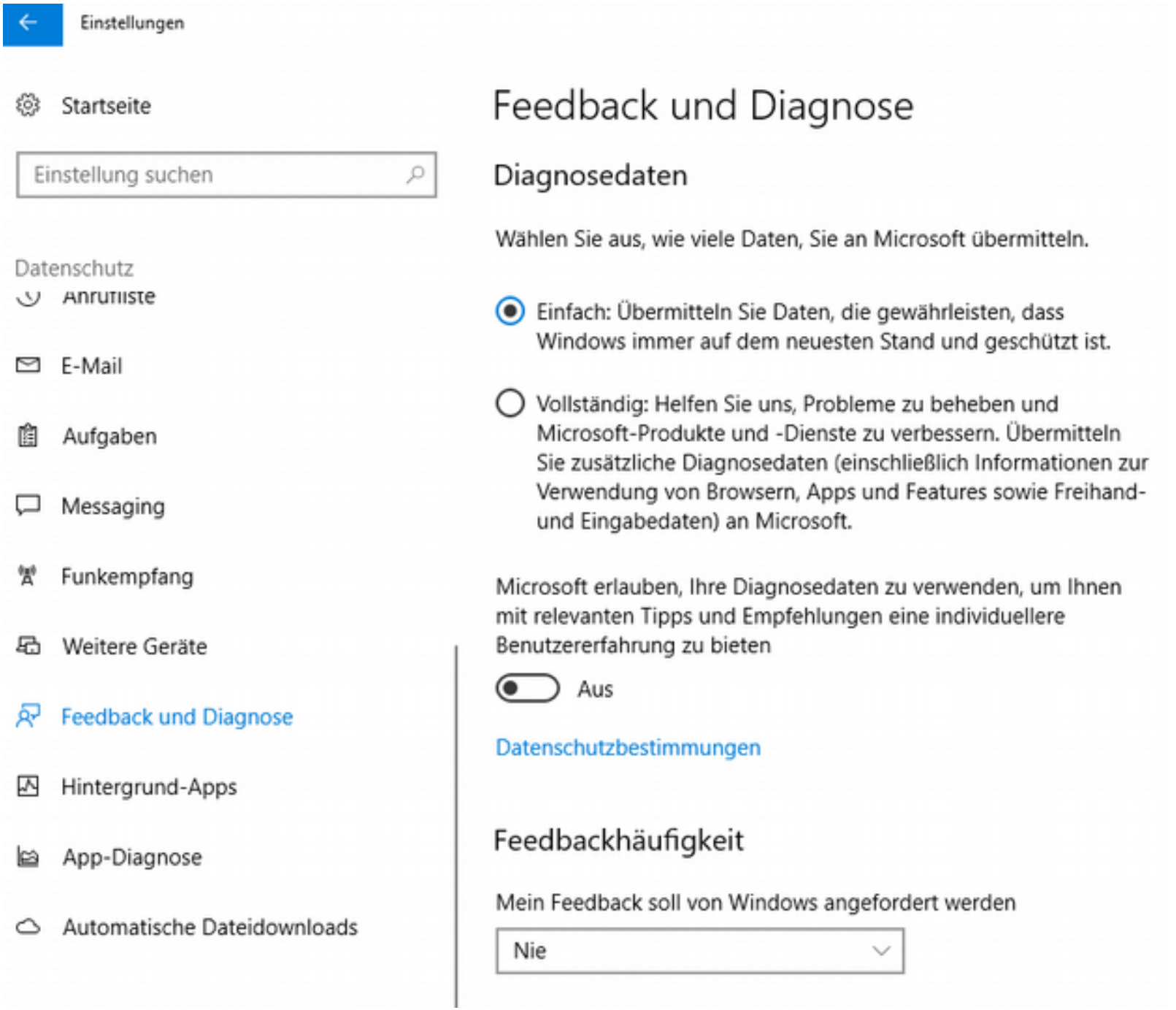
https://privacy.microsoft.com/de-DE/#introductionmodule

# Die sechs Datenschutzprinzipien des Nadella

- Volle Kontrolle über Ihre Daten
- Transparenz in Bezug auf die Erfassung und Verwendung von Daten
- Sicherheit: Wir schützen die Daten, die Sie uns anvertrauen, mit hohen Sicherheits- und Verschlüsselungsmaßnahmen
- Einsatz für den Schutz Ihrer Privatsphäre als fundamentales Menschenrecht
- Keine inhaltsbezogene Werbung: Wir nutzen die Inhalte Ihrer E-Mails, Chatprotokolle, Dateien oder sonstigen persönlichen Inhalte nicht für gezielte Werbung.
- Vorteile für Sie: Wenn wir Daten erfassen, nutzen wir diese in Ihrem Interesse zur Verbesserung unseres Angebots
- (Verkürzte Wiedergabe – Datenschutzprinzipien unter: https://privacy.microsoft.com/de-de/#introductionmodule)

# "Datenschutzalbtraum" Windows 10!

- Sammelwut lässt sich nur schwer verhindern
- Selbst wenn man in den Datenschutzeinstellungen das Senden sämtlicher Daten deaktiviert, werden dennoch Daten gesendet
- Als generelle Regel sollte gelten: Dienste, die Ihr nicht brauchet oder deren Aktionen Ihr nicht versteht, sollten deaktiviert werden



# Diagnose- und Nutzungsdaten = Vollständig

- Beispiele für Daten, die bei der Einstellung "Vollständig" von Win10 gesammelt und an Microsoft gesendet werden:
  - Daten über die Anwendungen, die auf dem Gerät installiert sind, beispielsweise Name, Version und Herausgeber der Anwendung
  - Browser-Nutzung, einschließlich Browserverlauf und Suchbegriffe
  - Teilweise Freihand- und Tastatureingaben (lt. Microsoft werden alle personenbezogenen Daten entfernt)
  - Erweiterte Fehlerberichterstattung, die den Speicherstatus des Geräts bei einem System- oder App-Absturz umfasst. Dabei können unbeabsichtigt Teile der Datei übermittelt werden, die Sie beim Auftreten des Problems verwendet haben
  - Datenweitergabe an OEM-Partner (z.B. Fehlerberichte)

https://privacy.microsoft.com/de-de/windows-10-feedback-diagnostics-and-privacy

# Schutz gegen den "Datenschutzalbtraum"

- Was könnt Ihr dagegen tun?
- Keine Tools oder 1-Click-Lösungen (z.B. O&O ShutUp10, DoNotSpy10)
- Einfach und nutzerfreundlich
  - Paper vom AKIF – Orientierungshilfe zur datenarmen Konfiguration von Windows 10, abrufbar unter: https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf
- Übergangslösung: So lang wie möglich bei einer älteren Windows-Version bleiben
- Auf Linux umsteigen; Windows nur noch für Programme nutzen, die unter Linux nicht laufen

# Windows 10 Report (September 2017)

- Windows 10 Enterprise (Build 14393 nach dem Creators Update, Build 15063) durch Bayerische Landesamt für Datenschutzaufsicht (BayLDA) in Ansbach
- Nach Standardinstallation 44 Einstellungen bzgl. Datenschutz
  - Noch immer massive Netzwerkaktivität
  - Beispiel: Entpacken einer Zip-Datei im Windows Dateibrowser (Explorer) löst Netzwerkverkehr aus
- **Schlussatz: "However, there is still no extensive guidance on how Windows 10 can be used in full compliance with European data protection law."**

https://www.lda.bayern.de/media/windows_10_report.pdf (in Englisch)

# Literaturempfehlung


- Arbeitskreis Informationssicherheit der deutschen Forschungseinrichtungen (AKIF) der Max-Planck-Gesellschaft, Orientierungshilfe zur datenarmen Konfiguration von Windows 10; Stand: 06.12.2016; abrufbar unter: https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf
- Mike Kuketz, Windows 10: Dem Konntrollverlust entgegenwirken; Stand: 28. März 2017; abrufbar unter https://www.kuketz-blog.de/windows-10-dem-kontrollverlust-entgegenwirken/
- Landesbeauftragter für Datenschut und Informationsfreiheit Baden-Württemberg, Sammlung an Informationen zur Datenschutz-Grundverordnung (DSGVO); abgerufen am 17.05.2018; abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/ds-gvo/

# Exkurs: Freie Software

- Freiheit 0: Die Freiheit, das Programm auszuführen, wie man möchte, für *jeden Zweck.*
- Freiheit 1: Die Freiheit, die Funktionsweise des Programms zu untersuchen und eigenen Bedürfnissen der Datenverarbeitung anzupassen.
- Freiheit 2: Die Freiheit, das Programm weiterzuverbreiten und damit seinen Mitmenschen zu helfen.
- Freiheit 3: Die Freiheit, das Programm zu verbessern und diese Verbesserungen der Öffentlichkeit freizugeben, damit die gesamte Gemeinschaft davon profitiert.

⇒ Viel mehr als Open Source (offenlegen der Quelltexte)

# Sichere Passwörter

# Sichere Passwörter (1)

Wie werden Passwörter geknackt?

- Brute Force
  - Alle möglichen Kombinationen ausprobieren
- Listen / Wörterbuch-Angriffe
  - Alle Wörter aus einer Liste oder einem Wörterbuch ausprobieren
- Social Engineering
  - Phishing, Person austricksen um PW zu erfahren
  - Gerne auch durch Facebook, LinkedIn etc.

# 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: »**D**er **B**all **i**st **R**und **&** **d**as **S**piel **d**auert **90** **M**inuten**!**«
- HausLocherTasteMeloneBagger
  - Wortreihung
- 2UrN47oCfK6jAZ8xuKHiop4upPsI73
  - Passwortgenerator

# Passwortverwaltung

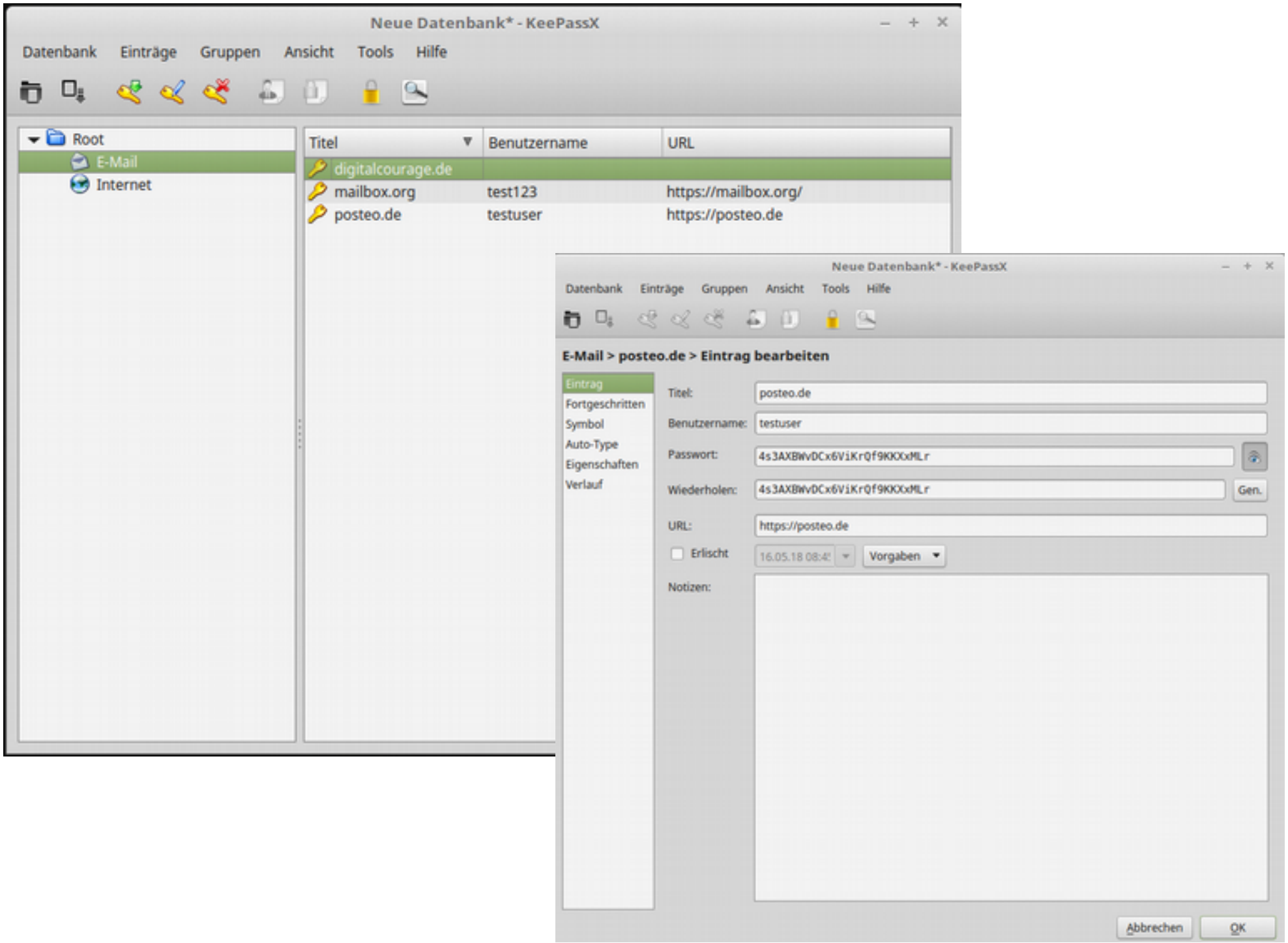
Software: **KeePassX**

## 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


Neue Datenbank* - KeePassX
Datenbank
Einträge
Gruppen
Ansicht
Tools
Hilfe
Root
E-Mail
Internet
Titel
Benutzername
URL
digitalcourage.de
mailbox.org
test123
https://mailbox.org/
posteo.de
testuser
https://posteo.de
Neue Datenbank* - KeePassX
Datenbank
Einträge
Gruppen
Ansicht
Tools
Hilfe
E-Mail > posteo.de > Eintrag bearbeiten
Eintrag
Fortgeschritten
Symbol
Auto-Type
Eigenschaften
Verlauf
Titel:
posteo.de
Benutzername:
testuser
Passwort:
4s3AXBWvDCx6ViKrQf9KKXxMLr
Wiederholen:
4s3AXBWvDCx6ViKrQf9KKXxMLr
Gen.
URL:
https://posteo.de
Erlischt
Vorgaben
Notizen:
Abbrechen
OK

# 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

# Dateiverschlüsselung

# Warum überhaupt verschlüsseln?

- Genereller Schutz sensibler und vertraulicher Daten
  - Bei Verlust/Diebstahl des Laptops oder USB-Stick
  - Jeder der personenbezogene Daten speichert
- Weil Ihr ein Grundrecht auf digitale Privats- und Intimsphäre habt!
  - Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
  - sog. IT-Grundrecht, Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG

# Dateiverschlüsselung

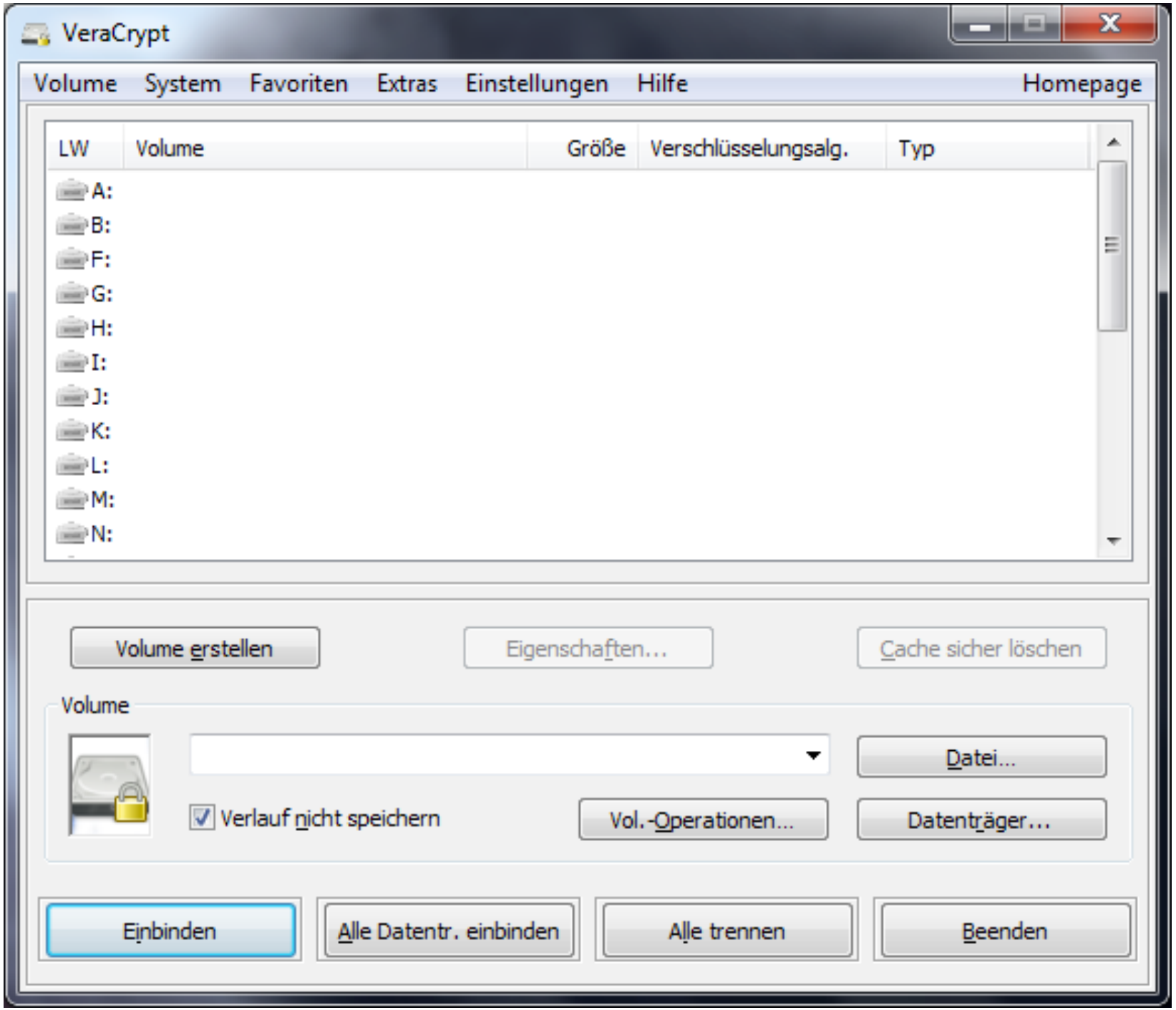

- Software: **VeraCrypt**
  - Software zur Dateiverschlüsselung
  - Quelloffen und auf allen gängigen Plattformen verfügbar
  - Freie Software

- Warum VeraCrypt?
  - Weil Windows-Verschlüsselung "BitLocker" vermutlich von Geheimdiensten geknackt werden kann

# Über VeraCrypt (1)

Was kann ich mit VeraCrypt verschlüsseln?

- Container (verschlüsselte Ordner)
- Datenträger:
  - Festplatten/SSDs
  - CDs, DVDs... (Container)
  - USB-Sticks
  - ...
- Systempartition



# Über VeraCrypt (2)

**Vorteile**

- Quelloffen, freie Software
- Nachvollziehbare Änderungen am Code
- Plattformübergreifend
- Auf USB-Stick transportierbar
- Unabhängiger Audit

**Nachteile**

- Komfortverlust
- Passwortverlust = Datenverlust

# Umgang mit VeraCrypt

- Was will ich verschlüsseln?
- Sicheres Passwort wählen
- Adminrechte notwendig
- Vorsicht bei fremden Geräten!
- Generell: Benutzerhandbuch zu VeraCrypt lesen

➔ Größtes Sicherheitsrisiko ist fast immer der Nutzer!

# Alternativen

- **dm-crypt** (Teil des Linux-Kernels ab Version 2.6)
  - z.B. Ubuntu und Mint erlauben Systemverschlüsselung bei Installation
- **7-Zip**: freie Software, unterstützt AES256-Verschlüsselung für 7z-Archive

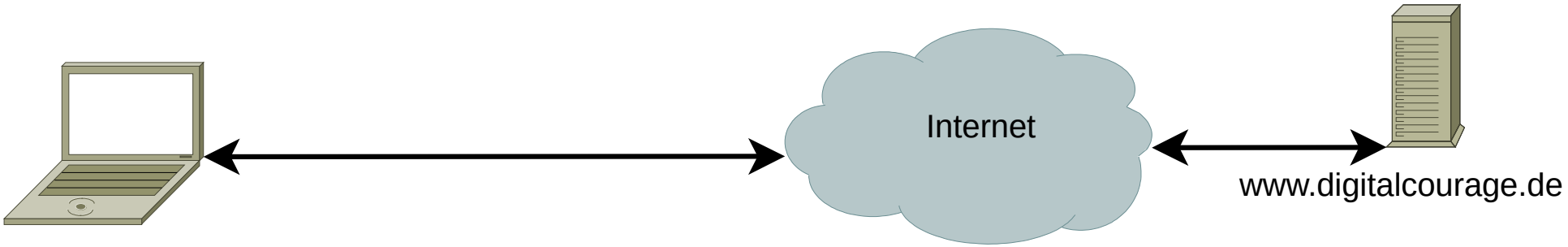
- Nicht vertrauenswürdig, da nicht quelloffen:
  - Windows: **BitLocker** (ab Vista, nur bei teuren Windows-Versionen)
  - MacOS: **FileVault**
  - Zahllose weitere kommerzielle Produkte

# Rechtliches

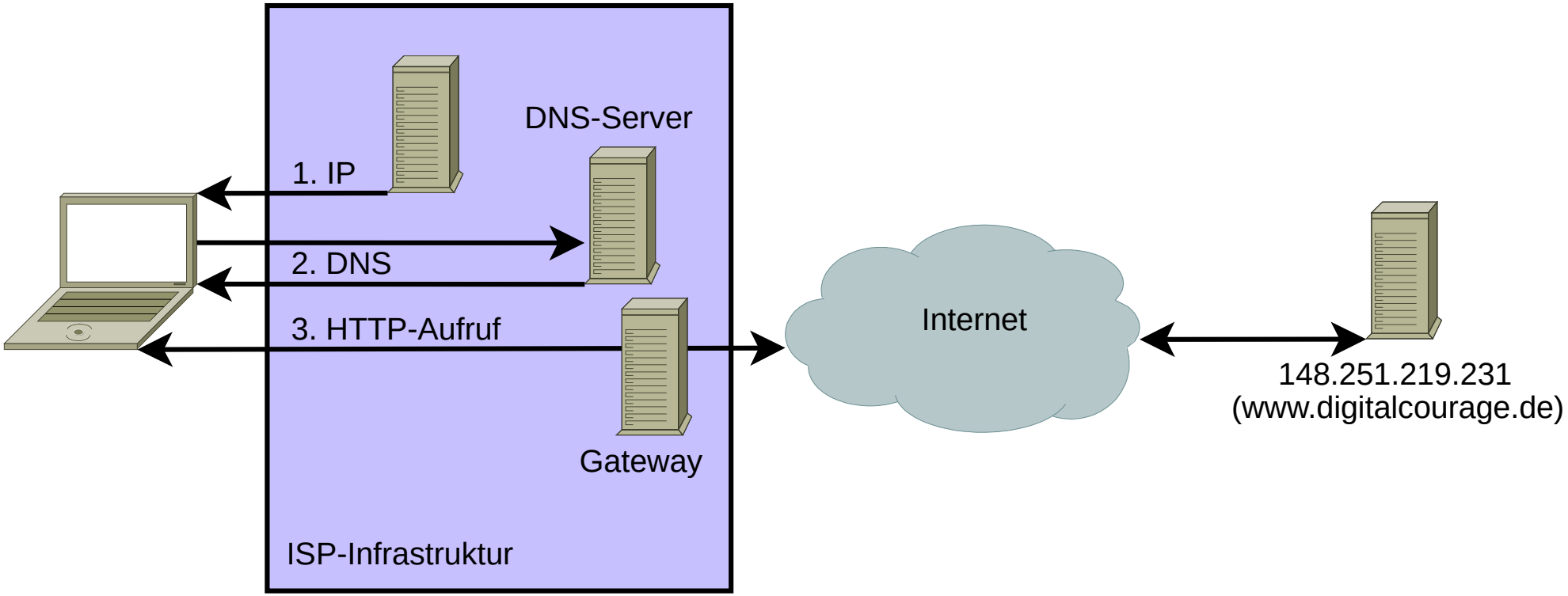
- Deutschland: Kein Zwang zur Herausgabe eines Passworts/Schlüssels bei möglicher Selbstbelastung
- Vorsicht im Ausland:
  - Großbritannien: Pflicht zur Herausgabe (→ RIPA), auch Beugehaft möglich!
  - USA: Ein- und Ausreise mit verschlüsselten Datenträgern problematisch

# Sicheres Surfen mit Privatsphäre

# Wie funktioniert der Aufruf einer Webseite?



# Was ist technisch *notwendig*?



# Wie schrecklich ist die Web-Realität?

Beispiel: www.spiegel.de

Standard-Firefox, Debian 9 GNU/Linux

# ... so schrecklich!

Beispiel: www.spiegel.de

Standard-Firefox, Debian 9 GNU/Linux

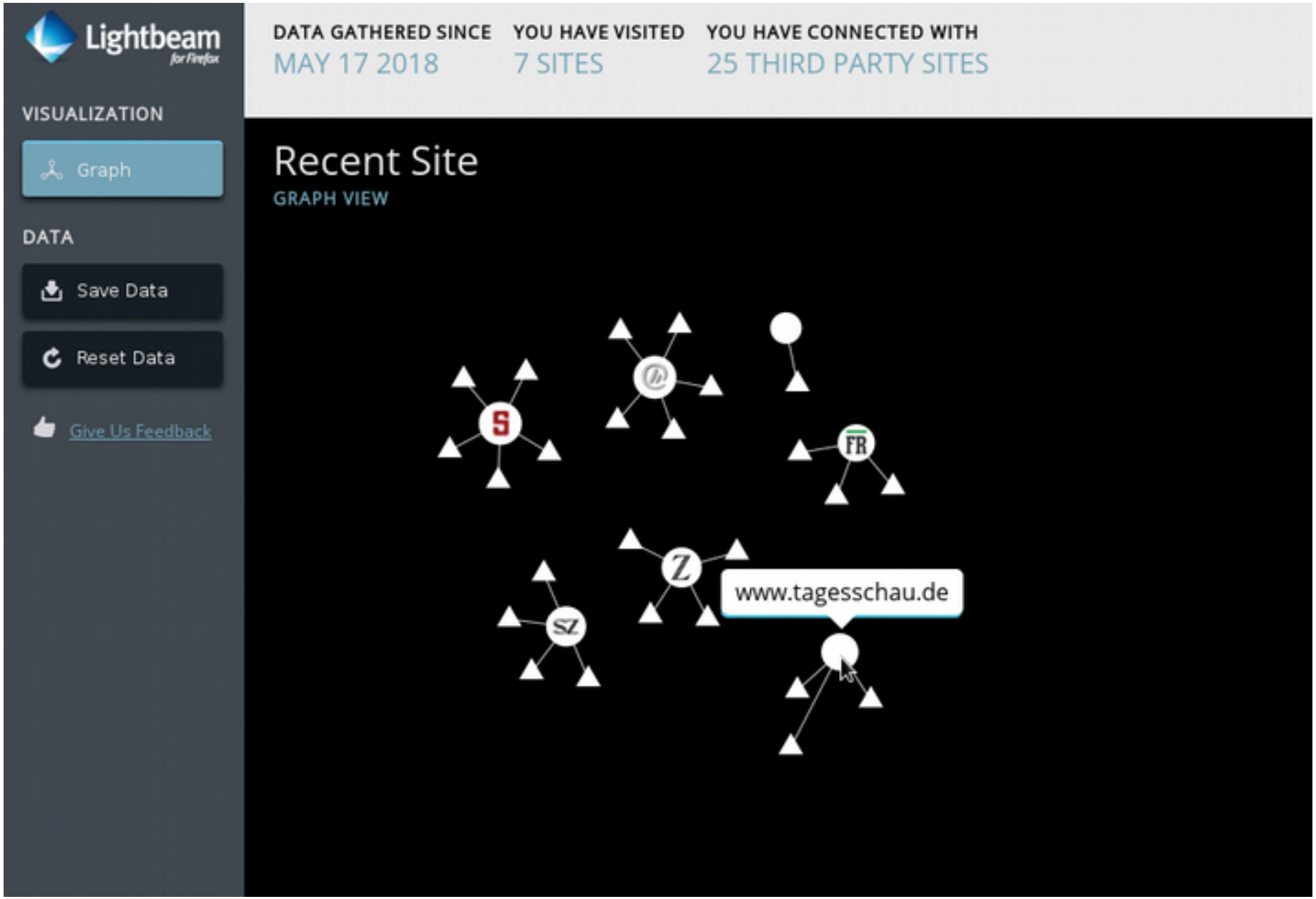
- 413-440 (nach 20s) HTTP-GETs an folgende Domains...
- Ablida.net, adition.com, adsrvr.org, atdmt.com, demdex.net, doubleclick.net, exactag.com, google.com, ioam.de, parsely.com, spiegel.de, t4ft.de, theadex.com, twiago.com, xplosion.de, yieldlab.net (ohne Subdomains)
- 8-10 MB; 59 Cookies von 24 Servern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

# Analyse im Firefox mit Lightbeam

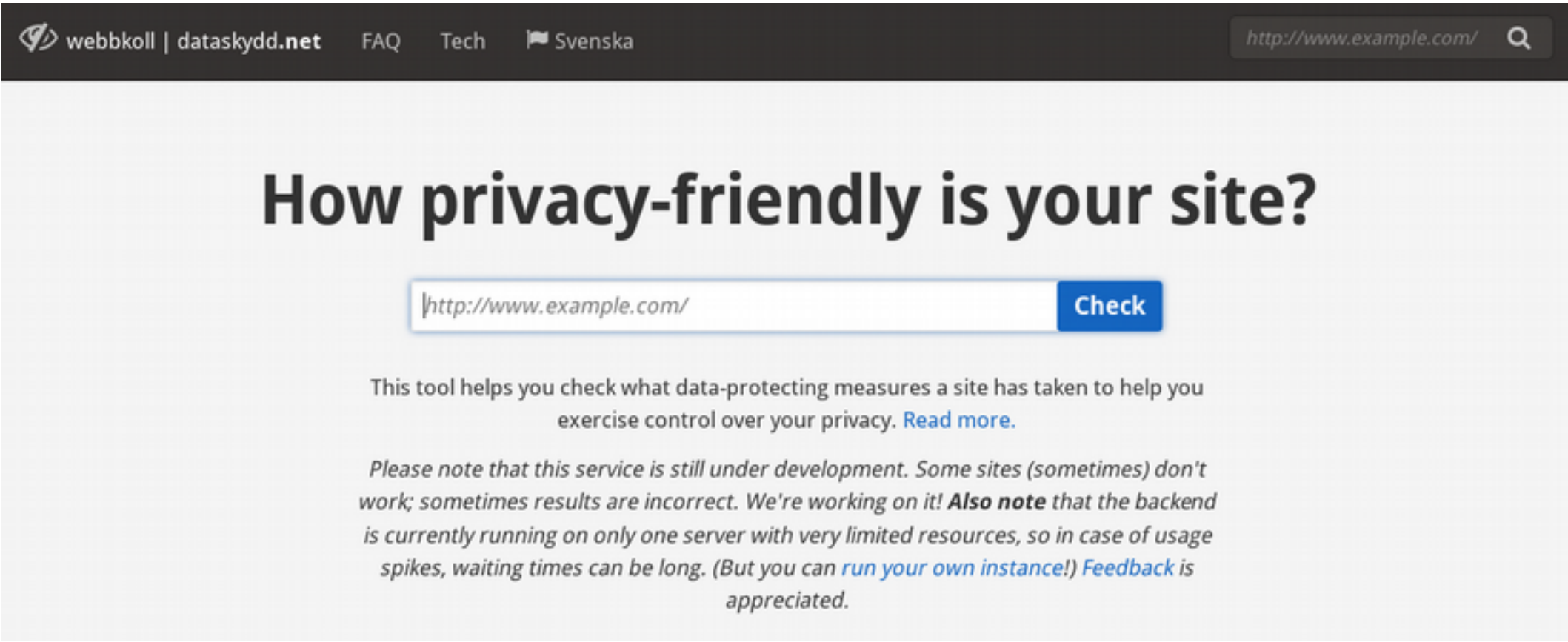



(Bild: CC-BY-2.0: EFF)

# Analyse im Firefox mit Lightbeam



# Einfach selber Testen mit Webbkoll




https://webbkoll.dataskydd.net/en

"How we take back the Internet?"

– Title of a TED Talk by Edward Snowden

# Sicheres Surfen mit Privatsphäre

Ziele:

- Sicherheit:
  - Vertraulichkeit
  - Authentizität
  - Integrität

# Sicheres Surfen mit Privatsphäre

Ziele:

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

# Sicheres Surfen mit Privatsphäre

Ziele:

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

# Sicheres Surfen mit Privatsphäre

Ziele:

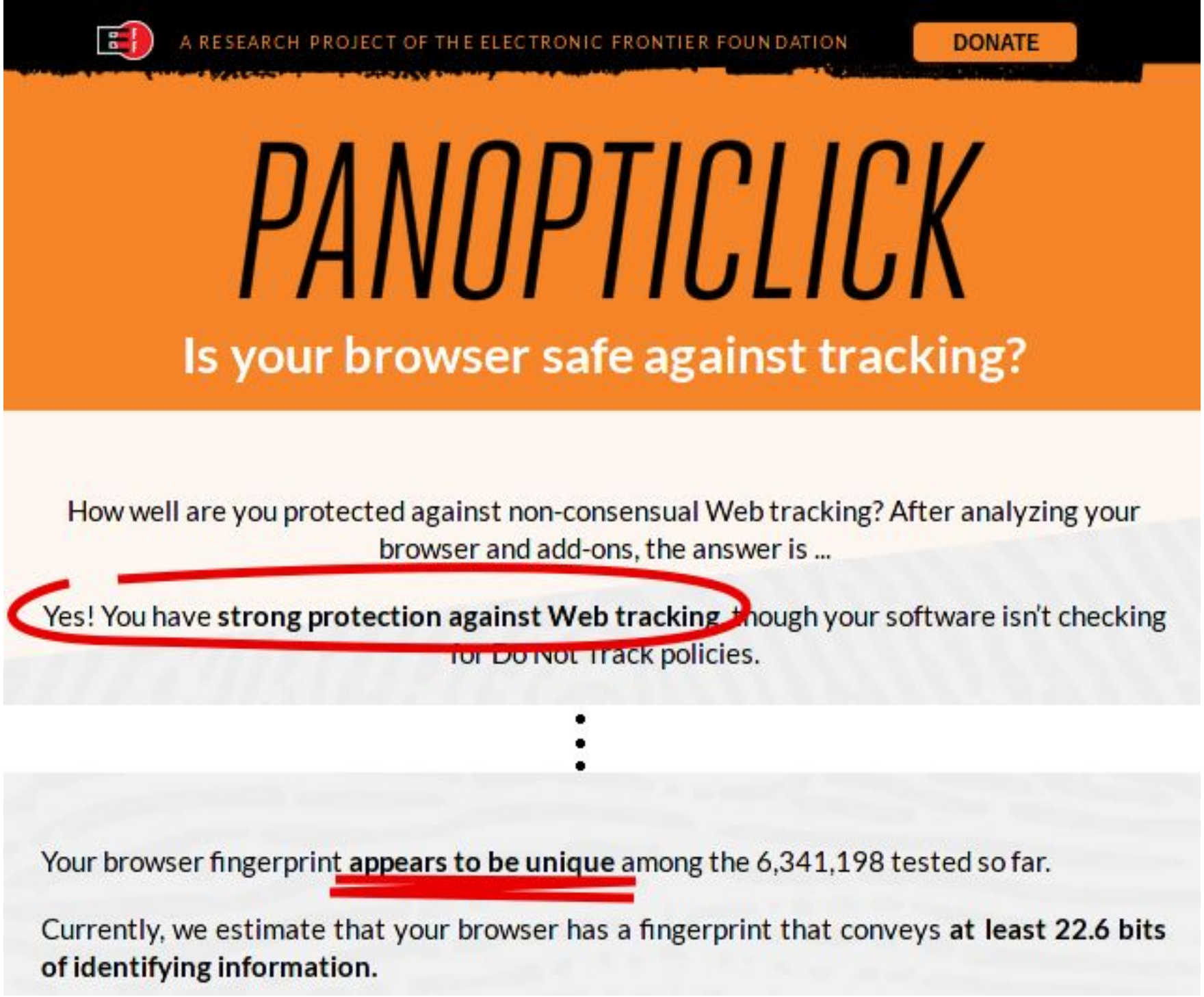
- Sicherheit:
  - Vertraulichkeit → HTTPS (Verschlüsselung)
  - Authentizität → HTTPS (Zertifikate)
  - Integrität → HTTPS
- Anonymität
  - Firefox
  - Tracking blocken → verschiedene Add-ons
  - Nur benötigte Cookies → Cookie-Einstellungen
  - IP-Verschleierung → Tor-Browser

# 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

- siehe https://panopticlick.eff.org/


A RESEARCH PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION
DONATE
PANOPTICLICK
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, ixquick.eu, DuckDuckGo.com, MetaGer.de, etc.
    (im Gegensatz zu Google auch keine individuellen 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

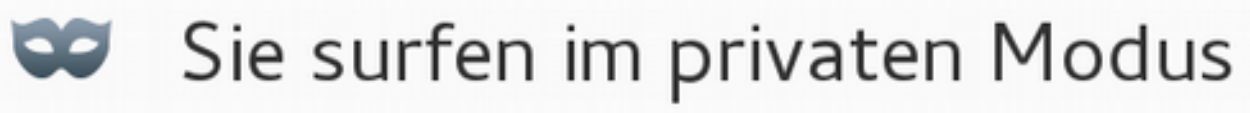
Wirkung von Add-ons und Einstellungen kontrollieren:

- 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



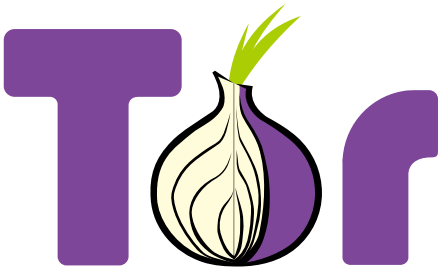
# WebRTC (statt Skype)

- 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/**

# Anonym surfen mit dem Tor-Browser

# Tor (von „The Onion Router“)



Was ist Tor?

- Netzwerk zur Anonymisierung von Verbindungsdaten
- IP-Adresse wird verschleiert

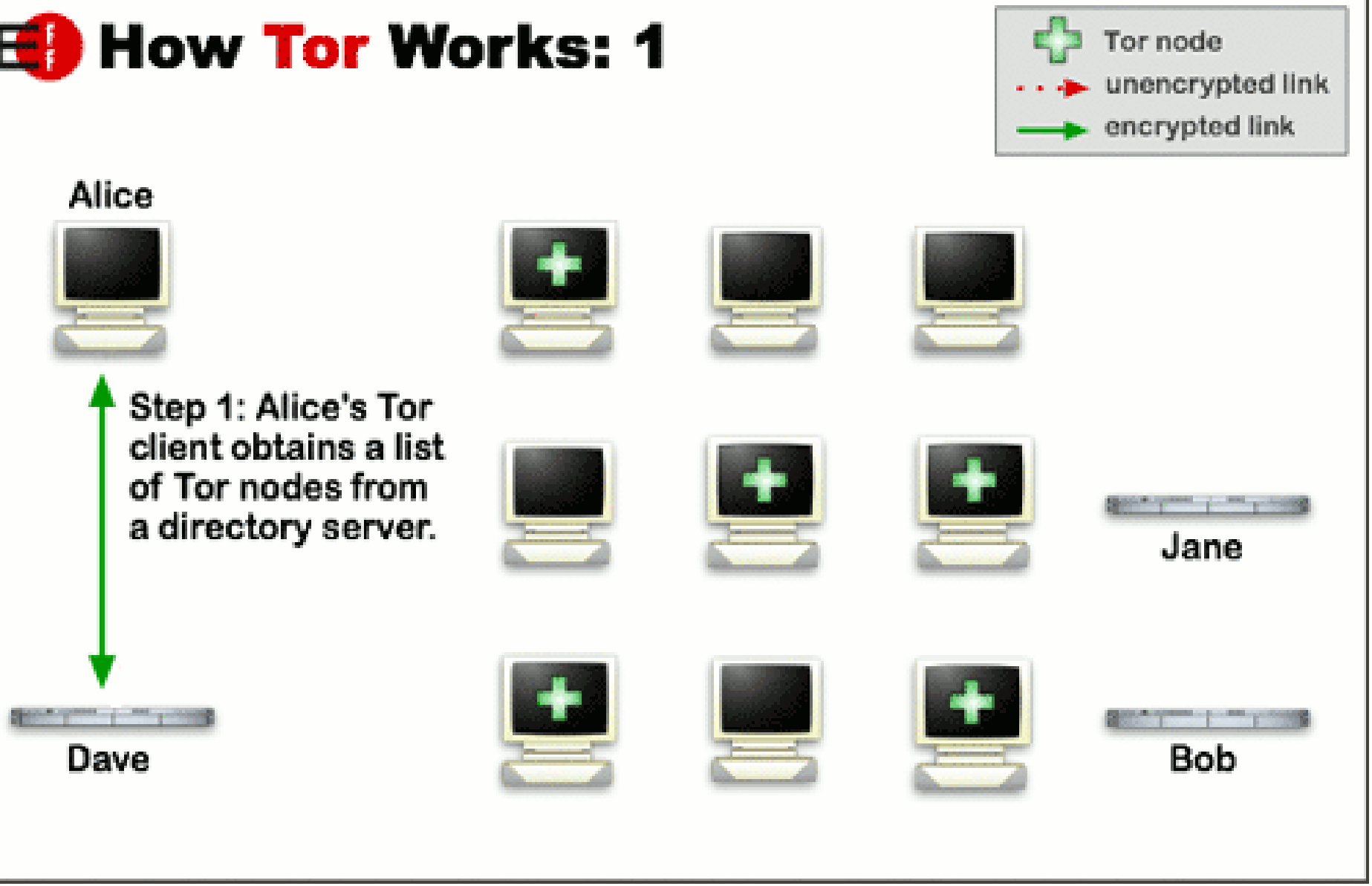
Vorteile

- Freie Software
- Anonymes Surfen

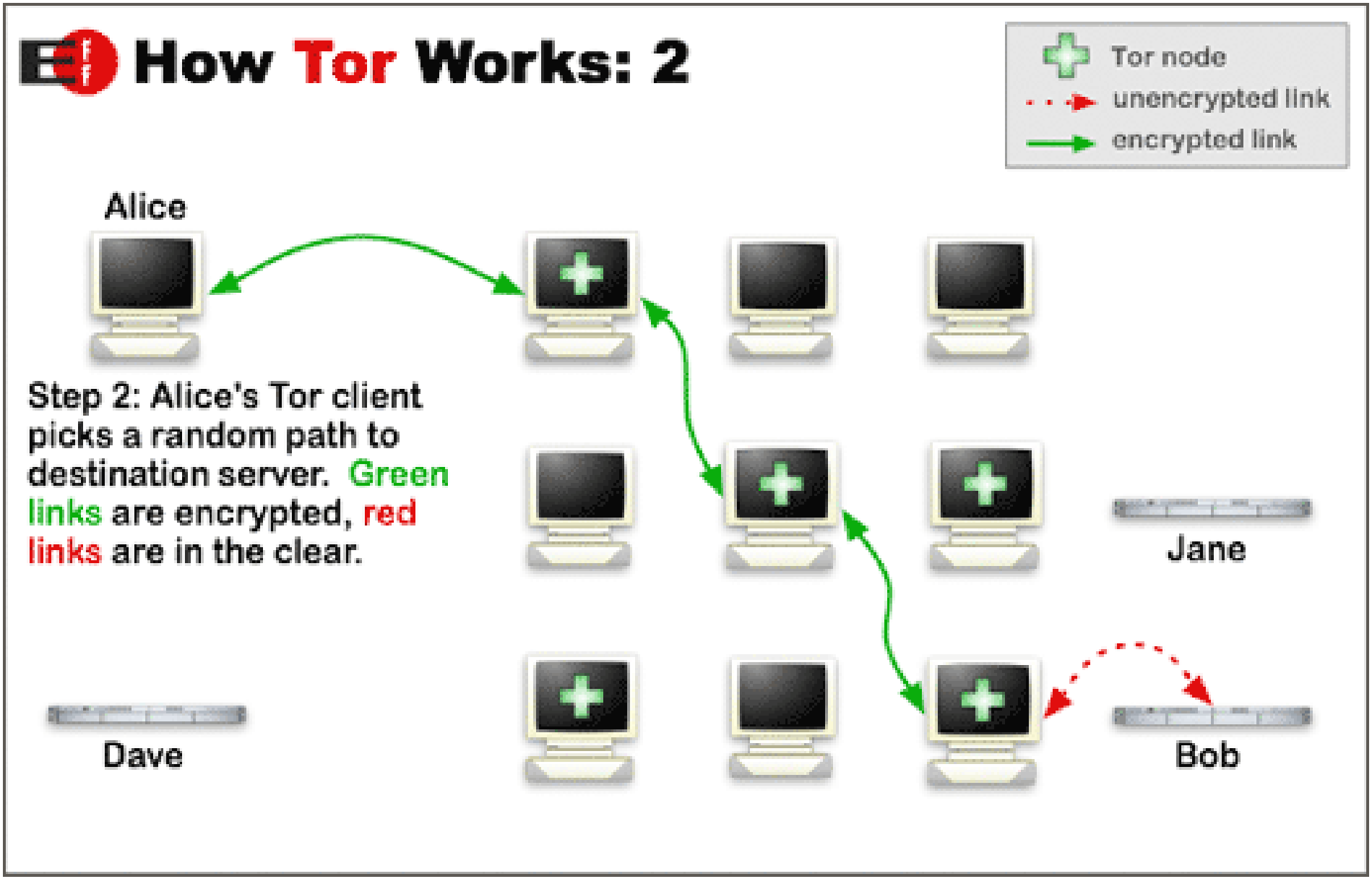
Nachteile

- Login bei personalisierten Seiten nicht sinnvoll
- Latenz ist größer

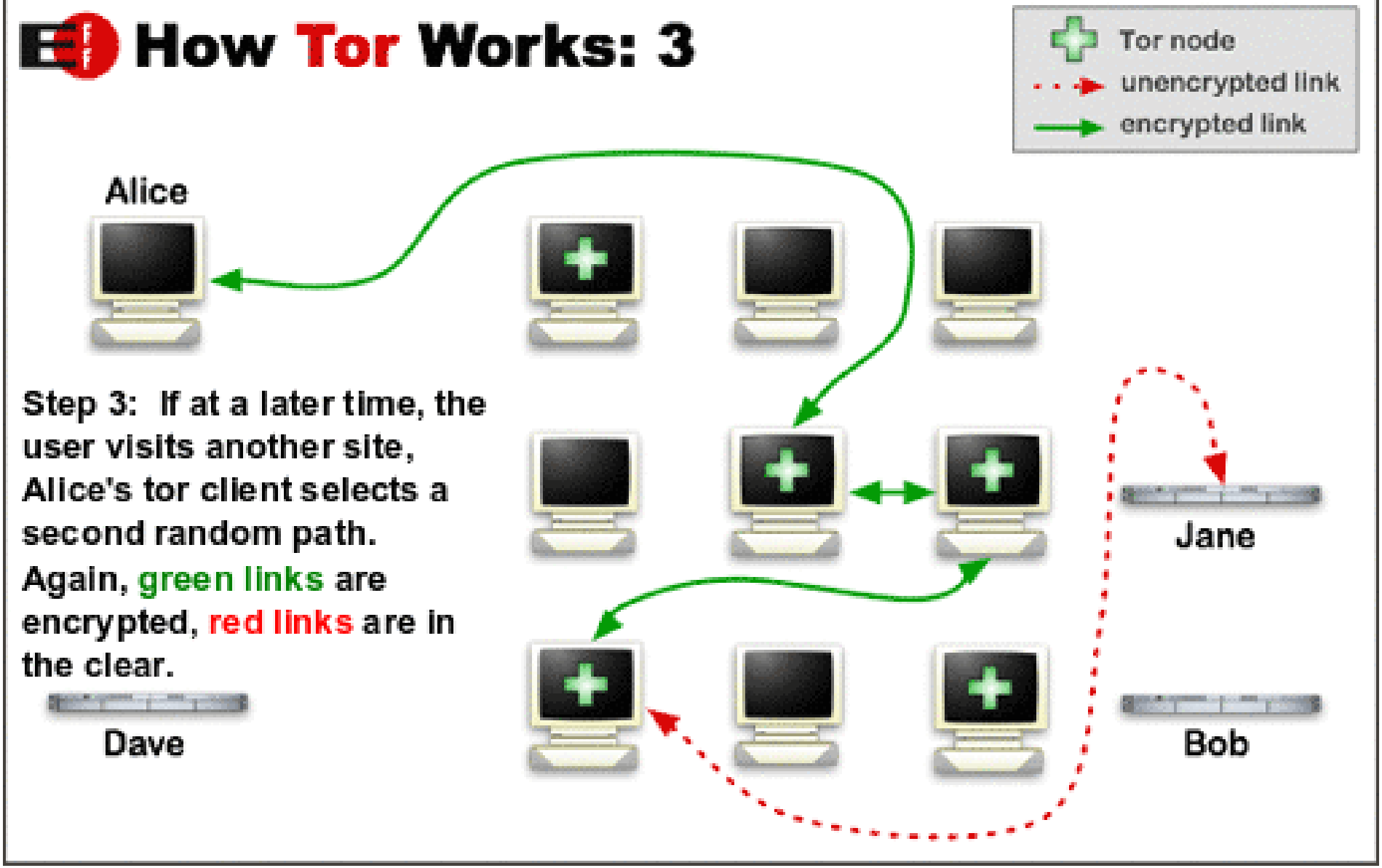
# How Tor Works: 1



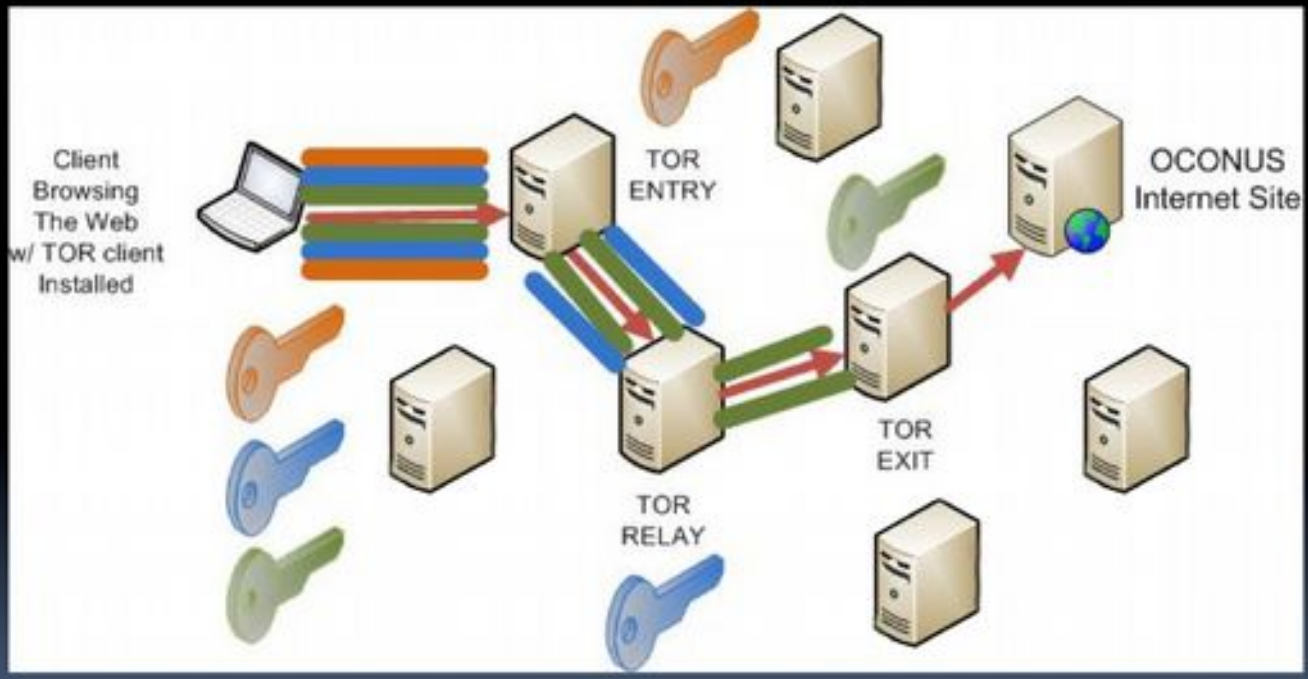
# How Tor Works: 2



# How Tor Works: 3

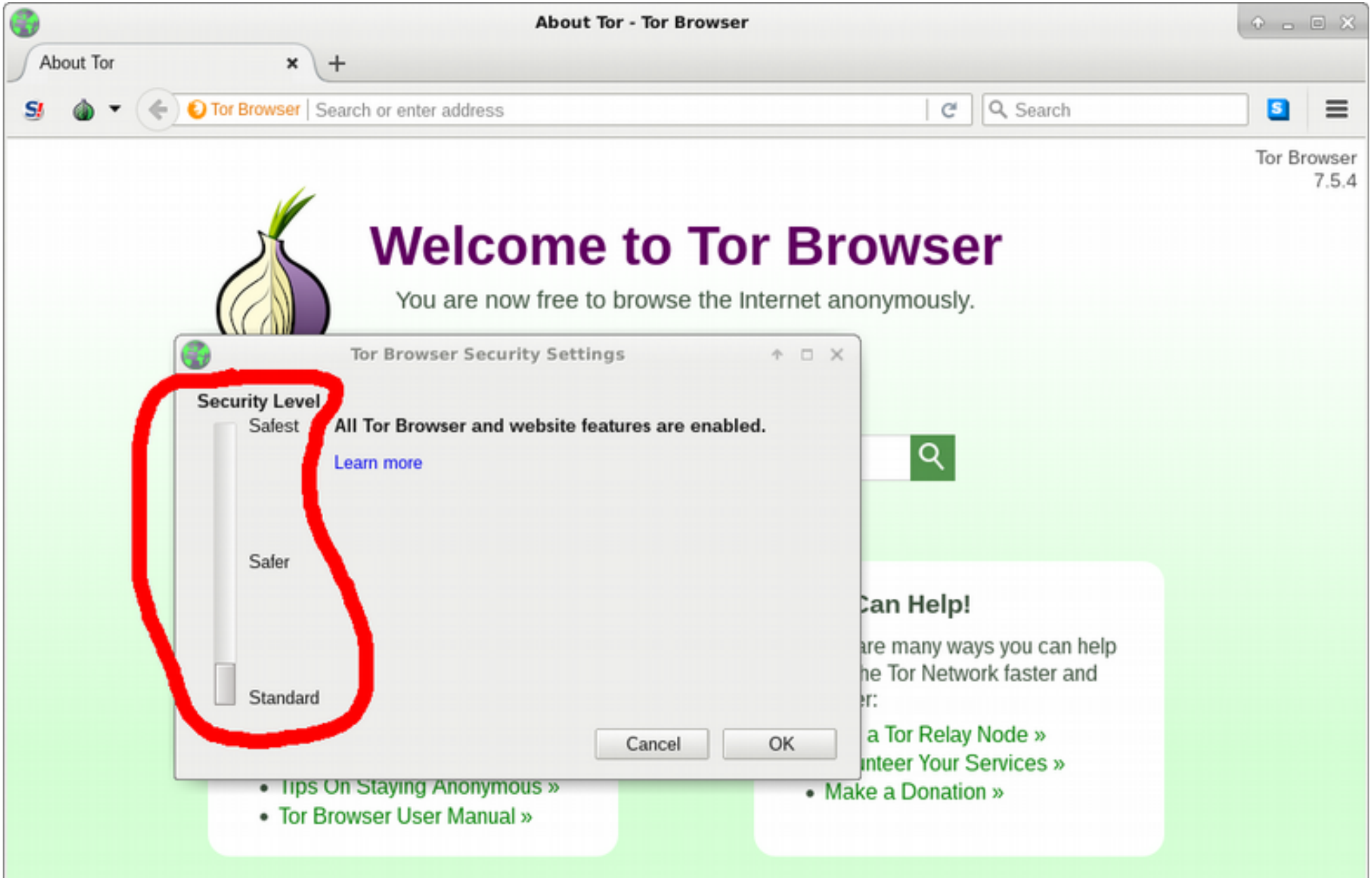


# (U) What is TOR?



# Tor-Browser

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


About Tor - Tor Browser
About Tor
Tor Browser
Search or enter address
Search
Tor Browser
7.5.4
Welcome to Tor Browser
You are now free to browse the Internet anonymously.
Tor Browser Security Settings
Security Level
Safest
All Tor Browser and website features are enabled.
Learn more
Safer
Standard
Cancel
OK
Can Help!
are many ways you can help
he Tor Network faster and
r:
a Tor Relay Node »
nteer Your Services »
Make a Donation »
Tips On Staying Anonymous »
Tor Browser User Manual »

# Tails – ein OS für Tor

**T**he **A**mnesic **I**ncognito **L**ive **S**ystem (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/

- Pause -

- Praxis -

# Agenda Freitag

| von | bis | Titel |
|---|---|---|
| 10:00 | 12:00 | Vortrag: Privatsphäre im Zeitalter der Massenüberwachung |
| 12:00 | 12:10 | - Kurze Pause - |
| 12:10 | 13:10 | Digitale Selbstverteidigung I<br>(W10, Passwörter) |
| 13:10 | 14:00 | - Mittagspause - |
| 14:00 | 15:30 | Digitale Selbstverteidigung II<br>(Datenträgerverschlüsselung, Browser) |
| 15:30 | 15:40 | - Kurze Pause - |
| 15:40 | 17:00 | Praxis |
| | | Open End |

# Agenda Samstag

| von | bis | Titel |
|---|---|---|
| 10:00 | 11:00 | Digitale Selbstverteidigung III (E-Mails) |
| 11:00 | 11:15 | - Kurze Pause - |
| 11:15 | 13:00 | Praxis |
| 13:00 | 14:00 | - Mittagspause - |
| 14:00 | 15:00 | Digitale Selbstverteidigung IV (Mobilgeräte) |
| 15:00 | 15:15 | - Kurze Pause - |
| 15:15 | 17:00 | Praxis |
| | | Feedback, Diskussion / Open End |