Unsere Forderungen:

- Meine Daten sollen keine Ware sein!
- Jede/r muss selbst bestimmen können, welche Daten wohin gehen dürfen.
- Apps haben sich an Rechte und Berechtigungen zu halten (Zweckbindung).
- Wir wollen kein gläserner Bürger sein.
- Daten-gierige Internetkonzerne müssen reguliert werden.
- Open Source - Creative Commons
  Jede öffentlich geförderte Software-Entwicklung muss Allen gehören.

Links:

Privatsphäre schützen	a-fsa.de/priv
Anonym und sicher	a-fsa.de/ano
Handy Datenschutz	a-fsa.de/handy
Open Source Programme	a-fsa.de/open
Privatsphäre-Buch	privacy-handbuch.de

Informieren Sie sich!
Bürgerrechtsarbeit kostet Geld – bitte unterstützen Sie uns mit Ihrer Spende!

Der Verein „Aktion Freiheit statt Angst e.V.“ engagiert sich als gemeinnütziger Verein im Bereich der Bürger- und Menschenrechte gegen Massenüberwachung und Sicherheitswahn und wir setzen uns ein für Informationsfreiheit und Netzneutralität.

Verteidigen wir gemeinsam unser Grundgesetz, unser Recht auf informationelle Selbstbestimmung und die Menschenwürde!

Jede/r kann mitmachen und sich mit uns für seine Bürgerrechte einsetzen.

Die Termine unserer regelmäßigen Treffen sind auf unseren Webseiten unter dem Punkt **Über uns/Treffpunkt** zu finden.

Aktion Freiheit statt Angst e.V.
Rochstr. 3,
D-10178 Berlin
Mail: kontakt@a-fsa.de
Web: www.a-fsa.de

A-FsA.de

AKTION FREIHEIT STATT ANGST

Spendenkonto: Aktion Freiheit statt Angst e.V.
IBAN: DE72 5003 1000 1060 9910 02
Triodos Bank, BIC: TRODDEF1

A-FsA ist seit 01.01.2011 nach §§ 52 1(2) Nr. 24 AO gemeinnützig, Spenden sind steuerlich absetzbar.

CO₂ NEUTRAL

AKTION FREIHEIT STATT ANGST

Für Freiheitsrechte, gegen Massen-überwachung und Sicherheitswahn

Mitglied im European Civil Liberties Network

Kein Profit aus unseren Daten

Meine Daten sollen keine Ware sein

Startpage statt Google,
Diaspora statt Facebook,
Threema statt WhatsApp,
Mastodon statt Twitter ...

Verteidigen wir den Grundsatz

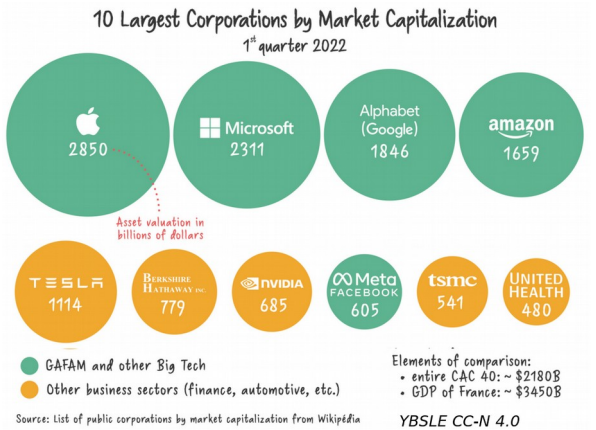
Private Daten schützen - öffentliche Daten nutzen

Deine Daten als Handelsware
Daten - das Öl des 21. Jahrhunderts

Viele Menschen wissen, dass Unternehmen mit dem Verkauf unsere Daten an Dritte Geld verdienen. Cyberkriminelle verkaufen das komplette digitale Leben einer Person für weniger als 50 Dollar – inklusive Daten von gestohlenen Social-Media-Accounts, Bankdetails oder Remote-Zugängen zu Servern oder den PCs und Tablets zu Hause.

Facebook existiert nur durch den Datenhandel und hat einen Marktwert von 600 Milliarden $. Bei Facebook werden Personen auf Fotos mit Gesichtserkennungssoftware identifiziert.

Studien zeigen, dass viele Apps sensible Nutzerdaten übertragen – meist ohne, dass diese für die Funktion der Apps notwendig sind. Wir sind gläsern und werden es in der Zukunft immer stärker.



Beispiele:

- Mein Smartphone weiß, wo ich wann und wie lange gerne bin.
- Die Post verkauft meine Adresse, Facebook meine "Likes".
- Meine Kundenkarten verknüpfen meinen Einkauf mit meiner Person, somit ist der Wert der Daten stets größer als der "Rabatt", den man Dir scheinbar gewährt.
- Der RFID Chip im Einkaufswagen regis triert ,was man länger anschaut und was man dann schließlich kauft.
- Die Folge ist personalisierte Werbung.
- Das „intelligente“ Kfz beobachtet dich und gibt deine Daten weiter. Die Folge kann eine teurere Versicherung sein oder der Beweis gegen dich beim Unfall.
- Die Weitergabe und Auswertung der Daten durch Versicherung, Schufa, u.ä. hat evtl. Jede/r selbst schon erlebt.
- Auch Gesundheits-Apps handeln mit meinen Daten
- und Alexa hört auf dem Nachttisch mit !

Ich möchte die Kontrolle über meine Daten behalten und nicht an unbekannte Konzerne zahlen.

Vorschläge:

- Vermeiden von Kreditkarte, EC-Karte, Bahncard, Kunden- und Rabattkarten,
- mehrere digitale Identitäten verwenden,
- nie dasselbe Passwort für verschiedene Webseiten oder Dienste verwenden,
- Passwortmanager nutzen, wie KeePassX
- Pseudonyme verwenden bei Accounts, und E-Mail Adressen,
- datenschutzfreundliche alternative Suchmaschinen nutzen: Startpage, Yacy,
- beim Surfen Anonymisierungsdienste, wie Tor oder Jondonym nutzen.
- Daten, die nicht gespeichert wurden, können auch nicht missbraucht werden.
- Verschlüsseln der Kommunikation mit Gnu/PG, Pretty Good Privacy, ...
- Offene App Stores, wie F-Droid / Free-Droid statt GooglePlayStore nutzen.

- Sichere Messenger nutzen, wie Wire, Conversations, Briar, Threema ... statt WhatsApp oder Telegram.
- VPNs (Virtual Privat Networks) nutzen
- Von Accounts und Blogs nach DSGVO das Löschen verlangen, wenn man sie nicht mehr braucht.
- Vertrauenswürdige E-Mail Provider nutzen: posteo.de oder mailbox.org statt Gmail, GMX, Freenet oder Web.de
- Für lokales E-Mail lesen Thunderbird oder K-Mail statt MS Outlook oder Apple Mail verwenden.
- Video-Messenger: Tox, Wire oder Jitsi statt Zoom, Facetime oder MS Teams
- Soziale statt asoziale Netzwerke, also Diaspora, Mastodon, Threema statt Facebook, Telegram, ...
- Zur Navigation Open Street Map, OSMand statt Google Earth, Apple Karten nutzen.
- Surfen mit Tor, Firefox oder Opera statt Chrome, Safari, MS Browser, ...
- Browser im privaten Modus nutzen.
- Auf dem Smartphone muss es nicht immer eine App sein. Viele Dienste sind auch über Webseiten erreichbar.