# Überwachung durch Unternehmen

## Inhaltsverzeichnis





Dr. Rainer Hammerschmidt, Vorstandsmitglied
MA Beate Baum, Wissenschaftliche Fachberatung

# Einleitung

**Wo lauern die Gefahren? Wie können wir uns schützen?**

Dies ist das Skript für eine Vortragsveranstaltung im Antikriegscafé COOP von **Aktion Freiheit statt Angst** am 14.3.2017

Wir dokumentieren hier die Inhalte des Vortrags und werden weitere Ergebnisse aus der anschließenden Diskussion demnächst hinzufügen.

Der Vortrag wurde von Uniwut Freies Fernsehen mitgeschnitten und wird demnächst, d.h.nach der Ausstrahlung durch den Offenen Kanal Berlin auch zum Download in unserer Mediathek und auf unserem Youtube-Kanal. zur Verfügung stehen.

Der erste Teil dieser Vortragsreihe "**Überwachung durch 'den Staat'** " ist unter folgendem Shortlink *a-fsa.de/d/17c* erreichbar

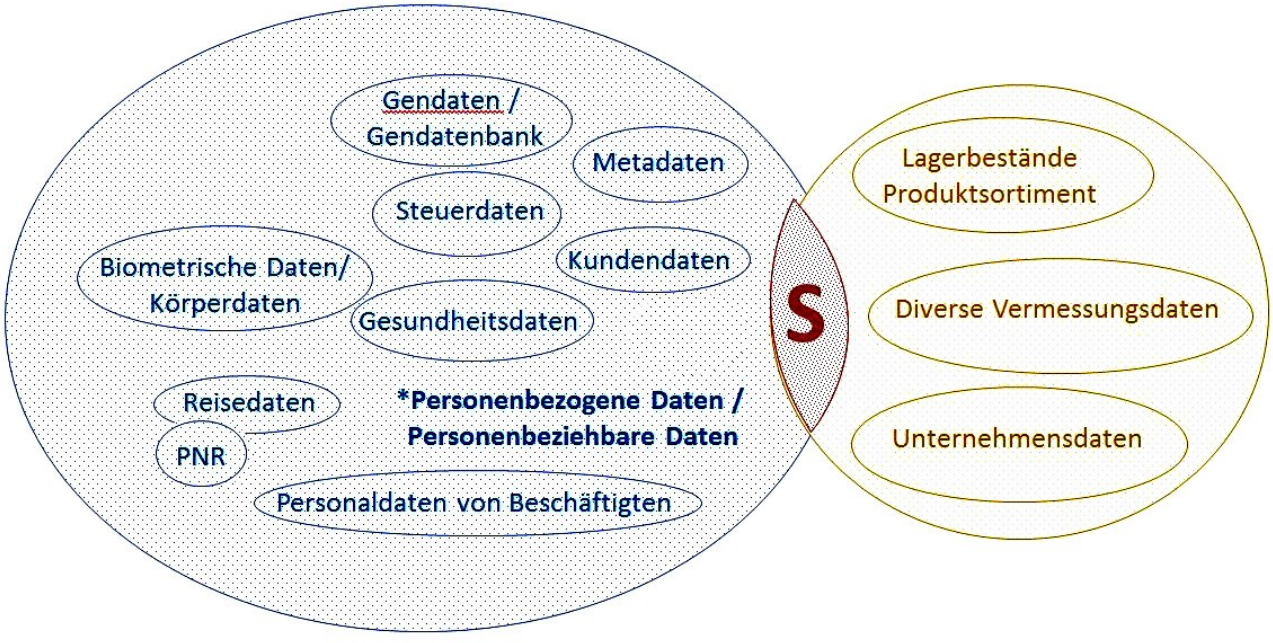
# Datenschutz – was ist das?

## Gesetze:

BDSG, Dez.1990
EU Datenschutz Richtlinie, 95/46/EG, Okt. 1995
EU Datenschutz Grundverordnung, Mai 2016

Kerninhalte:
Betrifft nur personenbezogene Daten
Anonymisierung und Pseudonymisierung von personenbezogenen Daten
BDSG ist ein Gesetz mit Erlaubnisvorbehalt (Gesetz, Verordnung, Einwilligung)

Damit ist jegliche Datenverarbeitung mit einem Personenbezug verboten, solange sie nicht durch Gesetz, Verordnung oder Einwilligung erlaubt wird.



Darstellung zur Unterscheidung von personenbezogene Daten und anonymen Daten - In der Schnittmenge befinden sich anonymisierte oder pseudonymisierte Daten.

## Grundprinzipien:

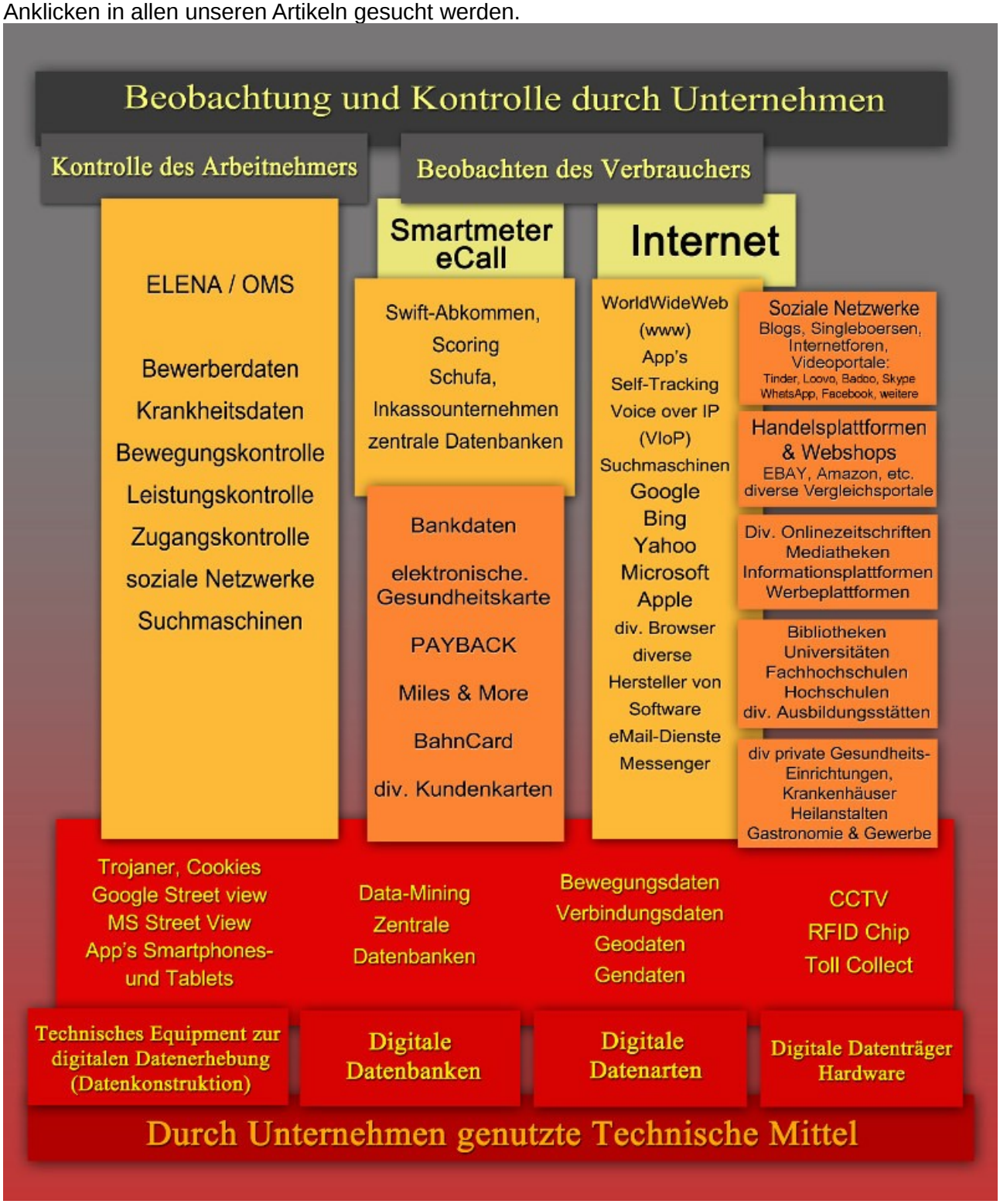
- Einwilligung (§4a)
- Datenvermeidung und Datensparsamkeit (§3a)
- Zweckbindung (§31,39)

Problem:
Datenschutz <> Privacy (nach US Recht)
Überwachung durch Unternehmen

## Wie wird der Bürger zum „gläsernen Bürger“?

Es geht diesmal nicht um „Sicherheit“ - sondern um Geld, viel Geld, wenn man sich die Unternehmenswerte der Internetgiganten ansieht.

Wir beginnen diesmal mit unserem Themenbaum "Wirtschaft". Dort können alle Begriffe durch Anklicken in allen unseren Artikeln gesucht werden.



Wir sehen eine Unterscheidung zwischen Unternehmenskontrolle und -überwachung gegenüber den eigenen Arbeitnehmern und gegenüber den Kunden - das sind wir alle, also praktisch alle Menschen.

Dazu gibt es eine Reihe von Begriffen, die Bereiche bezeichnen, in denen der Mensch dieser Kontrolle ausgesetzt ist, z.B. im Web, beim Surfen, in sozialen Netze, beim Einkaufen, bei der Berieselung durch Werbung. Und es gibt Bereiche, in denen er sich freiwillig dieser Überwachung aussetzt, z.B. im Smart Home, in eCall-befähigten Autos, auch bei seinen Gesundheitsdaten durch Tracking-Armbänder oder er lässt seine Kreditwürdigkeit berechnen.

## Arbeitnehmerdatenschutz

Es gibt kein Gesetz, alle Ansätze dazu wurden verhindert.

- Versuch durch Arbeitsminister Blüm wurde von der eigenen Partei verhindert
- Im 1. rot-grünen Koalitionsvertrag stand das Projekt drin, wurde nicht realisiert
- Im 2. rot-grünen Koalitionsvertrag war dieser Punkt verschwunden.
- Die FDP versuchte (glücklicherweise vergeblich) unter schwarz-gelb einen negativen Arbeitnehmerdatenschutz zugunsten der Arbeitgeber zu definieren.

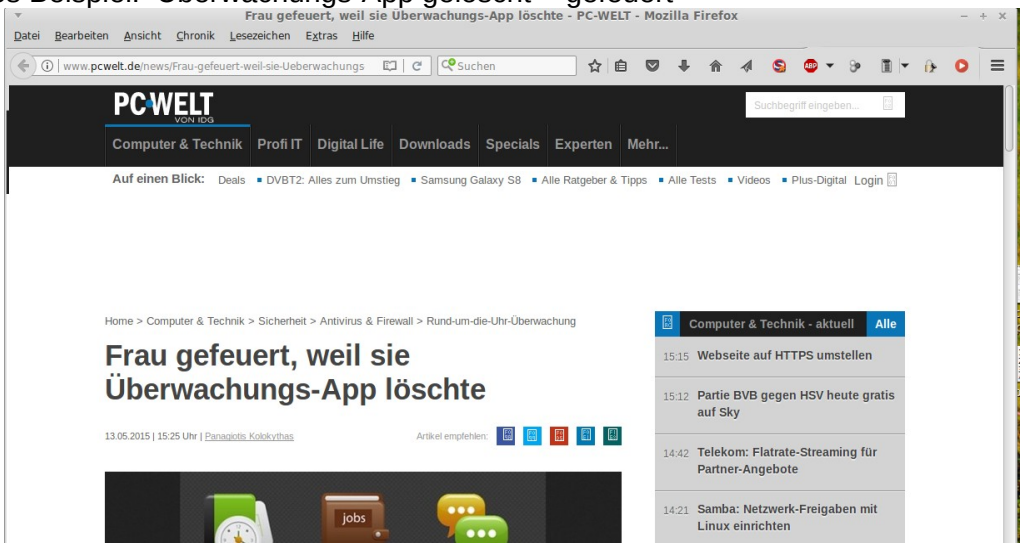
Ein Arbeitnehmerdatenschutz ist auch in der EU DS-GVO nicht enthalten. Das BDSG wird nun daran angepasst. Es gibt seit Jahrzehnten klare DGB Forderungen dafür. Zu regeln sind:

- Welche Daten sind zu schützen?


- Bewerberdaten
- Bewegungskontrolle
- Leistungskontrolle
- Zugangskontrolle
- Löschen der Daten nach dem Ausscheiden

Fazit: Es gibt keinen Arbeitnehmerdatenschutz - eine Überwachung von Beschäftigten ist z.Zt. nur durch die Betriebsräte mit Hilfe des Betriebsverfassungsgesetzes (BetrVG) zu verhindern.

Die Folge sind viele Überwachungsskandale in Betrieben.
Ein krasses Beispiel: Überwachungs-App gelöscht - gefeuert



Der Artikel berichtet über die Software Xora Stree tSmart von Clicksoftware, sie überwacht dich Tag und Nacht. Eine Frau wurde gefeuert, nachdem sie eine App auf ihrem Smartphone gelöscht hat, die ihre Bewegungen rund um die Uhr überwachte. Die Frau hatte keinerlei Probleme mit der Überwachung während der Arbeitszeit gehabt. Da sie sich aber in der Freizeit wie eine Gefangene mit einer elektronischen Fußfessel gefühlt habe, deinstallierte sie schließlich die App.

http://www.pcwelt.de/news/Frau-gefeuert-weil-sie-Ueberwachungs-App-loeschte-Rund-um-die-Uhr-Ueberwachung-9668969.html
und https://www.aktion-freiheitstattangst.org/de/articles/4949-20150514-frau-gefeuert-weil-sie-ueberwachungs-app-loeschte.htm

# Vorschriften machen uns zu „gläsernen Bürgern“

- **Elektronische Gesundheitskarte**,
- bisher Kosten über 6 Mrd. Euro
- bisher außer dem Foto ohne Funktion, erste Funktionen sollen bis 2018 implementiert werden
- Es gibt 380.000 Apps für den individuellen Gesundheitszustand,
- Der Vorsitzende der TK, sieht darin eine große Chance. „Bei den Krankenkassen seien diese sensiblen Daten gut aufgehoben.“
- In Großbritannien wurde ein ähnliches Projekt nach Kosten von 6 Mrd. Euro abgebrochen.
- ELGA, die elektronische Gesundheitsakte läuft in Österreich und der Schweiz

- **Elektronischer Gehaltsnachweis** (ELENA)
- damit solten alle monatlichen Gehalts- Lohn- und Hartz-IV Zahlungen in eine gemeinsame Datenbank geschrieben werden
- nach Milliardeninvestitionen -> gestorben
- Nachfolgerprojekte sind BEA (gewesen) und OMS

- **Steuer-ID** - damit dürfen die Finanzämter alle Konten abfragen
- und dies wird auch ausgiebig getan

- **SWIFT** , ein europäisches Buchungssystem in Belgien kennt alle Überweisungen in/aus der EU
- die USA dürfen darauf nach dem Safe Harbor Abkommen zugreifen
- Safe Harbor wurde vom EuGH für unsicher und nichtig erklärt
- der Nachfolger von Safe Harbor ist Privacy Shield und hat die gleichen Lücken
- die Zusicherung, das EU Bürger nun in den USA auf Herausgabe der Daten klagen können hat Präsident Trump in einem Dekret wieder abgeschafft

- **Schufa-Abfragen** (es gibt viele Schufa-ähnliche Firmen, die unsere Daten sammeln, z..B. das Hinweis- und Informationssystem der Versicherer (HIS)
- die Schufa darf fast alles wissen, wir aber nicht ihre Algorithmen

Die Schufa will mit Hilfe des Hasso-Plattner-Institut der Universität Potsdam (HPI) bei Facebook und anderen Internetquellen Daten über Verbraucher sammeln. Damit will sie die von ihr errechneten sogenannten persönlichen Schufa-Scores verbessern. Allein in Deutschland gibt es rund 20 Millionen Facebook-Nutzer deren Daten dadurch zur Schufa fließen könnten.

Dann kann die Schufa eine Rasterfahndung über 20 Millionen Menschen in Deutschland machen, die einen Facebook oder Twitter Account besitzen. Man erwartet, dass man dadurch Menschen findet, die über plötzliches Geldvermögen prahlen, ab 9000€ könnte ein Mord in der Verwandtschaft oder im Bekanntenkreis dahinter stecken.

http://www.spiegel.de/netzwelt/web/schufa-will-kreditdaten-bei-facebook-sammeln-a-837454.html
und http://www.sueddeutsche.de/digital/versuchte-facebook-twitter-analysen-was-uns-die-schnueffel-schufa-lehrt-1.1376581
und https://www.aktion-freiheitstattangst.org/de/articles/2943-20120608-schnueffel-schufa-und-facebook.htm

Diese Beispiele lassen sich zu Hunderten finden. Eine Kategorisierung ist schwer und es ist nie eindeutig ob es Fahrlässigkeit oder Kriminelle Energie war, um mehr Daten zu bekommen. Wir haben es im folgenden mit 3 Kategorien versucht.

# Fahrlässigkeit – Kriminelle Hacks – Unzulänglichkeiten

## Fahrlässigkeit

- Telekom-Gehälter u.a. Daten von 120.000 Mitarbeiter im Netz sichtbar
- https://www.aktion-freiheitstattangst.org/de/articles/3833-20130904-datenpanne-veroeffentlicht-telekom-gehaelter.htm
- Daten von Millionen ADAC Mitgliedern im Netz
- https://www.aktion-freiheitstattangst.org/de/articles/5241-20151103-daten-von-19-millionen-adac-mitgliedern-lesbar.htm
- WDR: Patientenakten vom Nachbarn lesen durch einfachen Telefonanruf bei einer Kasse
- https://www.aktion-freiheitstattangst.org/de/articles/5473-20160330-patientenakten-vom-nachbarn-lesen.htm
- Paypal kündigt seinem Kunden wegen Ende-zu-Ende-Verschlüsselung

*Was*? Ein Unternehmen kündigt einem Kunden, weil dieser Wert auf Sicherheit legt?

Der Grund für die jetzige Kündigung sei die "Ende-zu-Ende-Verschlüsselung, die zur Folge habe, dass unerkennbar ist, was sich auf der Plattform befindet."

https://www.aktion-freiheitstattangst.org/de/articles/4811-20150301-paypal-mag-nur-offene-kunden.htm
und https://www.golem.de/news/umstieg-auf-bitcoin-paypal-kuendigt-dotcoms-mega-wegen-verschluesselung-1502-112634.html

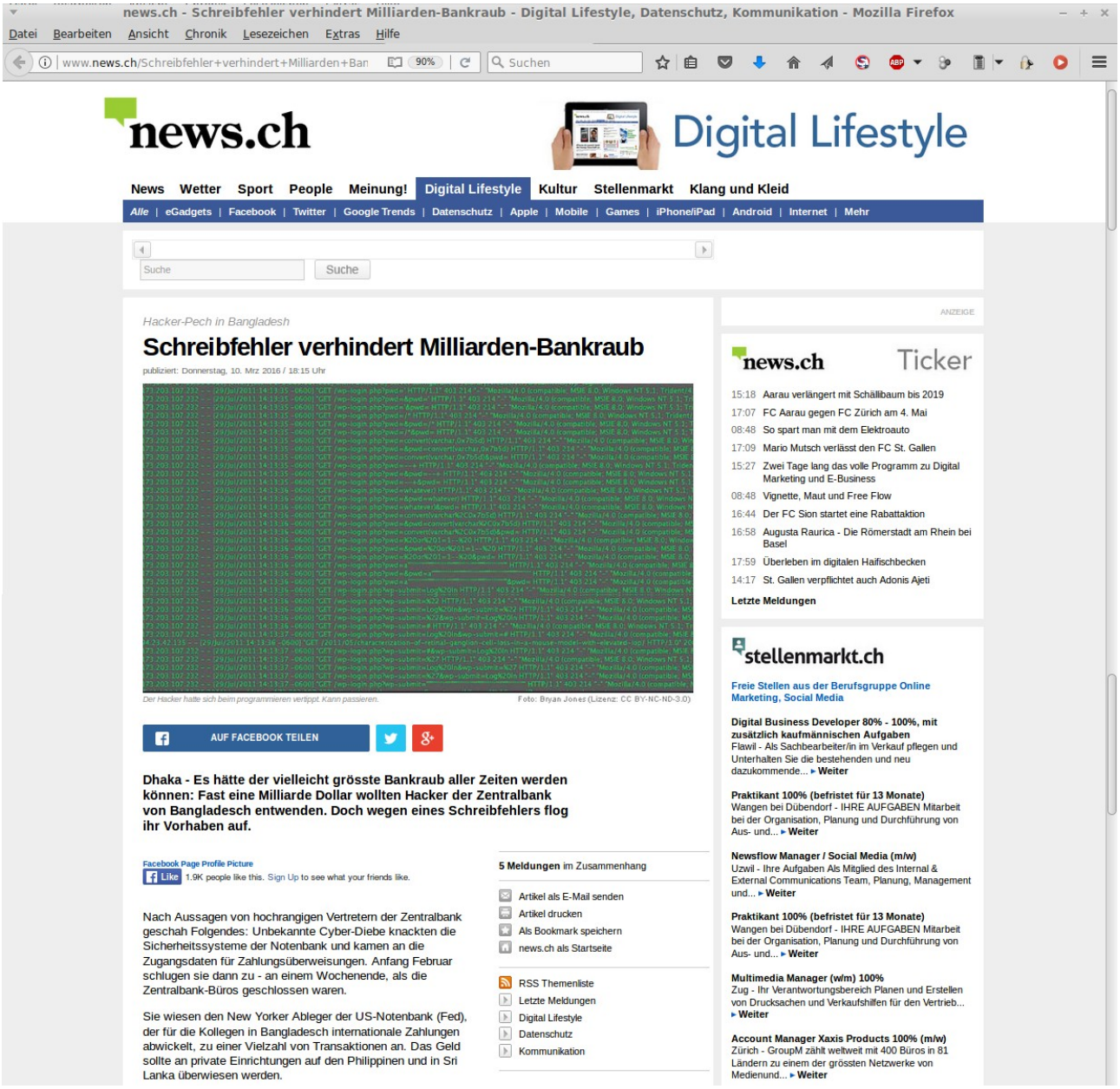
## Kriminelle Hacks

Insgesamt verlieren deutsche Unternehmen durch Wirtschaftsspionage 11,8Mrd€/J, ein großer Teil richtet sich auch und in großem Maß gegen nicht personenbezogene Daten ...

- Handy ausgeschaltet – denkste!
- Vermeintlich ausgeschaltetes Smartphone hört mit
- https://www.aktion-freiheitstattangst.org/de/articles/4796-20150221-handy-ausgeschaltet-denkste.htm
- Verschlüsselungstool verschlüsselt nicht sondern fotografiert den Nutzer
- https://www.aktion-freiheitstattangst.org/de/articles/4879-20150410-verschluesselungstool-verschluesselt-nicht.htm
- TaschenlampenApp kopiert das Adressbuch
- https://www.aktion-freiheitstattangst.org/de/articles/4036-20131207-taschenlampen-app-strahlt-nur-nach-aussen.htm
- Telekom Vorstand spioniert den Betriebsrat aus,  Opfer der Telekom-Spitzelaffäre wollen Akteneinsicht
- https://www.aktion-freiheitstattangst.org/de/articles/1193-20100321-staatsanwaltschaft-laesst-zumwinkel-und-ricke-laufen.htm
- Bahn sammelt Krankendaten von Mitarbeitern  (wieder Zweckbestimmung verletzt!)
- https://www.aktion-freiheitstattangst.org/de/articles/483-20090804-bahn-sammelte-auch-krankendaten-von-mitarbeitern.htm
- Yahoo: 500 Millionen Kontendaten entwendet (wohl eher 1 Mrd.)
- https://www.aktion-freiheitstattangst.org/de/articles/5746-20160924-yahoo-nutzer-sollten-ihren-account-pruefen.htm
- https://www.aktion-freiheitstattangst.org/de/articles/5765-20161009-yahoo-verliert-wohl-eine-milliarde.htm
- Online Banking ist nicht sicher
- Online Banking wird wieder unsicherer: von der normalen TAN Liste zur  iTan, zur mTan über 2 Wege war gut, jetzt wieder Zusammenführung auf einem(!) Smartphone
  - Schutzsystem von N26 Online-Bank komplett ausgehebelt
  - Tesco Bank registriert gleichzeitig 20.000 illegale Abbuchungen
  - Datenleck: Commerzbank tauscht 15.000 Kreditkarten
  - Schreibfehler verhindert Milliarden-Bankraub (nur 81 Mio geklaut)

http://www.news.ch/Schreibfehler+verhindert+Milliarden+Bankraub/690784/detail.htm
und https://www.aktion-freiheitstattangst.org/de/articles/5444-20160311-schreibfehler-verhindert-milliarden-bankraub.htm

Insgesamt sind trotzdem Online über die Jahre schon eine Milliarde Dollar  gestohlen  worden. Die Banken sind gegenüber geschädigten Kunden kulant, um das Vertrauen in das unsichere System nicht zu verspielen. Und auch wenn sich die Milliarde riesig anhört, muss man bedenken, dass die Banken für ihre Kunden allein bei den berüchtigten CumEx Geschäften die Finanzämter, also uns Steuerzahler, um 10 Milliarden Euro erleichtert haben.




## Technische „Unzulänglichkeiten“

- Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) warnt vor dem Einsatz von Windows 10
- in jedem Fall empfiehlt es den Flash-Player auszuschalten,
- https://www.aktion-freiheitstattangst.org/de/articles/4751-20150126-bsi-raet-flash-player-ausschalten.htm
- "Windows 10 ist wie eine Abhöranlage" warnt die Verbraucherzentrale Nordrhein-Westfalen
- https://www.aktion-freiheitstattangst.org/de/articles/5426-20160301-windows-10-ist-wie-eine-abhoeranlage.htm
- Forscher haben gemessen, dass Windows 10 in 8h über 55000-mal "nach Hause telefoniert",
- Von den konnektierten Hosts waren 51 dem Unternehmen Microsoft zuzuordnen, die überwiegende Anzahl von 113 Verbindungen zu "fremden Mithörern" war nicht zu

ermitteln .

- https://www.aktion-freiheitstattangst.org/de/articles/5400-20160213-windows10-telefoniert-5500-mal-am-tag.htm
- Die BSI Warnung wird scheinbar ernst genommen: Die US Atom U-Boote laufen weiter unter Windows XP .
- Dazu hat das US Verteidigungsministerium einen Sonder-Supportvertrag mit Microsoft, da XP nicht mehr gewartet wird.
- https://www.aktion-freiheitstattangst.org/de/articles/5367-20160125-atomkrieg-weiter-mit-windowsxp.htm
- Die US-Wahlcomputer sind in Minuten manipulierbar .
- Durch Einstecken einer vorbereiteten PCMCIA Karte in den offen zugänglichen Slot lässt sich ein beliebiges Wahlergebnis erzeugen .
- https://www.aktion-freiheitstattangst.org/de/articles/5923-20170222-wahlcomputer-in-minuten-manipulierbar.htm
- der CCC hat niederländische Wahlcomputer in Zeiten unter einer Minute gehackt .
- Keyless Cars erfreuen die Autoschieber
- So berichtet der ADAC, dass 20 Autotypen leicht knackbar sind in dem man das Schlüsselsignal kopiert .
- https://www.aktion-freiheitstattangst.org/de/articles/5457-20160319-keyless-cars-erfreuen-die-autoschieber.htm
- Vom Fernseher und Handy zu Hause ausspioniert
- Bluetooth-Schlösser senden Passwort im Klartext
- Ein Leuchtmittel wird zum Lauschmittel .


http://www.spiegel.de/netzwelt/gadgets/samsung-warnt-vor-eigenen-smart-tv-geraeten-a-1017447.html

und https://www.aktion-freiheitstattangst.org/de/articles/4777-20150210-vom-fernseher-zu-hause-ausspioniert.htm

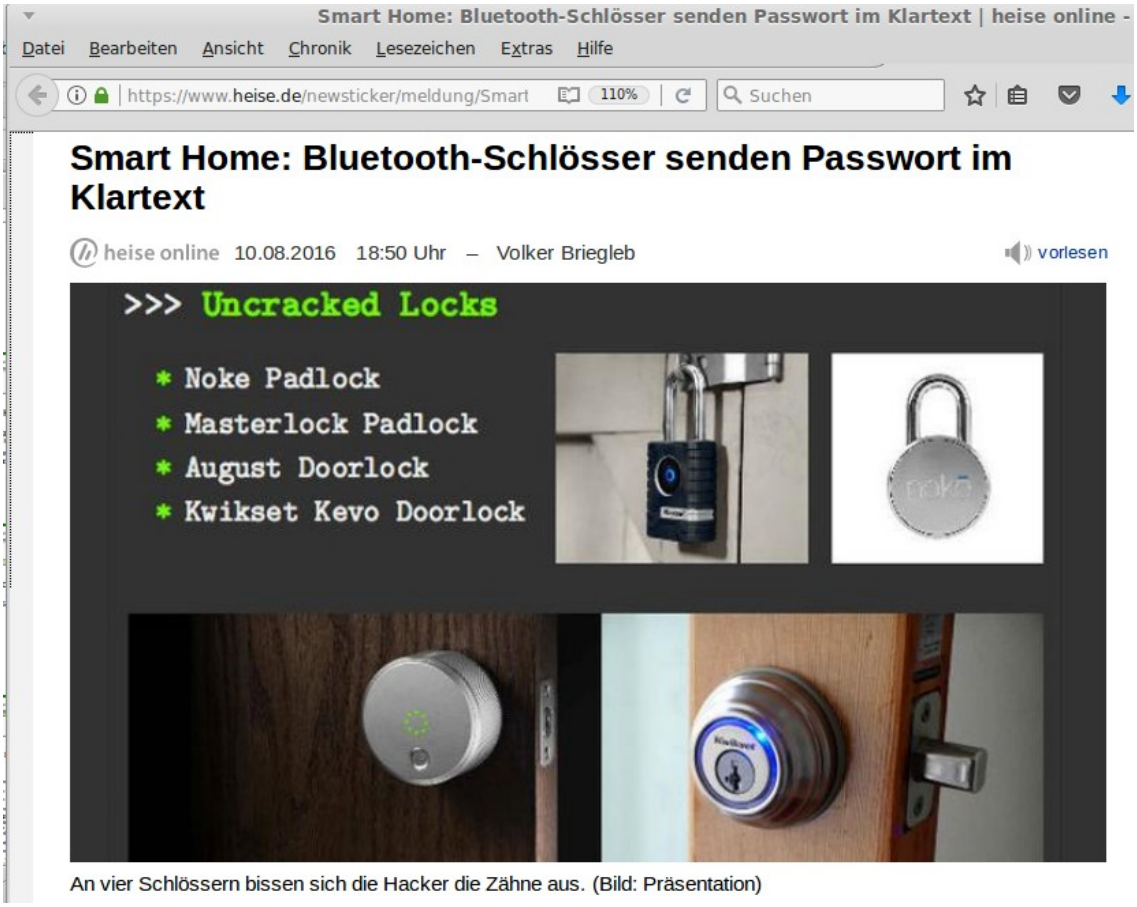
Das Gleiche gilt auch für die ständigen Zuhörer Alexa, Siri, die Puppe Cayla, ..

Der Fernseher kann dann auch noch persönliche "Minuspunkte" vergeben, wenn er bemerkt, dass wir bei bestimmten Werbeeinblendungen einfach dazwischen reden. So lässt sich die Akzeptanz von Werbung leicht kontrollieren.

Besonders perfide wird es, wenn eine Gerätebrücke aktiv wird. Beim sogenannten Cross Device Tracking, gesendet z.B. durch einen Werbespot mittels eines nicht hörbaren Ultraschallsignal, wird dieses Signal durch ein im Raum liegenden Smartphone oder Tablet verarbeitet, wenn die entsprechende App darauf installiert ist. Mit Cross Device Tracking ist eine eindeutige Identifizierung des Nutzers möglich, auch wenn er eigentlich verschiedene Inhalte/Partner nur über verschiedene Geräte ab- oder anruft.

https://www.datenschutzbeauftragter-info.de/cross-device-tracking-nutzerverfolgung-vs-datenschutz/
und https://www.aktion-freiheitstattangst.org/de/articles/5630-20160624-fernseher-redet-mit-dem-handy.htm

Das CIA Interesse an Samsung Fernsehern ist seit einigen Wochen durch die Wikileaks Veröffentlichungen bekannt.
https://www.aktion-freiheitstattangst.org/de/articles/5944-20170309-wikileaks-cia-schnueffelt-in-unseren-haushaltsgeraeten.htm



An vier Schlössern bissen sich die Hacker die Zähne aus. (Bild: Präsentation)

Alle getesteten Bluetooth-Schlösser, außer den 4 hier abgebildeten empfangen ihre Passwörter im Klartext.
http://www.heise.de/newsticker/meldung/Smart-Home-Bluetooth-Schloesser-senden-Passwort-im-Klartext-3292041.html
und https://www.aktion-freiheitstattangst.org/de/articles/5696-20160816-bluetooth-schloesser-senden-passwort-im-klartext.htm

Wer solche Risiken umgehen möchte, kann sich auch in seinem Handgelenk einen kleinen RFID-Chip implantieren lassen, um bestimmte Funktionen im Gebäude, wie das Tür öffnen oder die Bedienung des Kopierers zu steuern. Ein High-Tech-Bürokomplex in Schweden bietet dies ab sofort seinen Mitarbeitern an. Hoffentlich können diese auch "nein" sagen ...

RFID Chip im Arm sind inzwischen auch in spanischen Ferienclubs zum Bezahlen gängig. So hat man ein zeitloses Andenken an seinen Urlaub ...

Lineup der Sengled-Birnen. Sengled Voice ist die zweite Birne von links. (Bild: Daniel AJ Sokolov)

So wie man mit der Haustür sprechen kann, geht es auch mit der „Glühbirne“: Leuchtmittel wird Lauschmittel
http://www.heise.de/newsticker/meldung/CES-2016-Gluehbirne-hoert-mit-3056853.html
und https://www.aktion-freiheitstattangst.org/de/articles/5336-20160101-leuchtmittel-wird-lauschmittel.htm

Jederzeit ist das Abhören möglich. Das gilt auch für Alexa, Siri, Puppe Cayla oder im Auto, ...
Die Bundesnetzagentur verbietet erstmals ein Spielzeug, denn die Puppe Cayla ist nicht als Sendeeinrichtung erkennbar - das ist in Deutschland verboten!
https://www.aktion-freiheitstattangst.org/de/articles/5922-20170221-puppe-cayla-getarnte-sendeanlage-im-kinderzimmer.htm

# Bewegungsprofile und Verhaltensmuster

## Mögliche Aufnahme und Speicherung unserer Gespräche


- durch Smartphone, Tablet, Laptop, ...
  - liefert Geo- bzw. Verhaltensprofile
  - nimmt unsere Gespräche auf (Siri, Alexa, Cayla, …)
  - beim Einkaufen speichert es unsere Vorlieben
  - daraus entsteht mittels Scoring ein digitales Abbild
- ebenso beim Surfen im Netz,
  - z.B. erzeugt der Aufruf der Webseite bild.de
    2339 Verbindungen zu 195 Hosts
  - nur 13 davon gehören dem Besitzer der aufgerufenen Seite,
  - 182 sind fremde Hosts mit denen wir in keiner Weise kommunizieren wollten.
  - Alle haben Zugriff auf unsere IP, Browserdaten, … und kennen unser Surf-Ziel.
  - Das sind Verbindungen zu Unbekannten und wir tragen die Kosten!
- Wir tragen die Kosten von durchschnittlich 600MB/Tag,
  - beim Smart-TV hört der Rückkanal mit
  - Kühlschränke haben schon Spam-Mails verschickt
  - die "Abhör“-Puppe Cayla u.ä. kennen wir schon

Wir versenden unsere Geo- und Verhaltensprofile oder speichern freiwillig unsere Daten in Clouds, von denen wir nicht wissen, wer sonst noch Zugang zu den Daten hat, beim Einkaufen durch Payback und andere Kundenkarten geben wir unsere Gewohnheiten preis. Für uns ist dies ein "Datenverlust", für den Empfänger bares Geld. Durch Scoring kann er uns weiter "abzocken" in dem er unser digitales Abbild geschickt in seine Verkaufsstrategien einbaut.

Google Maps mag komfortabel sein, aber wir geben unser Bewegungsprofil an einen Internetgiganten. Eine weltweite Karte gibt es auch als Open Data. Open Street Map hat zumindest in Europa und den USA die gleiche Qualität im Kartenmaterial und wir können sicher sein, da wird nichts gespeichert.
Auch Abmahnungen bei von Google Maps genutzten Karten sind häufig sobald man bei der richtigen Quellenangabe im Web nicht aufpasst.

## Bewegungsprofile und Verhaltensmuster II

Wenn wir unterwegs sind, wird es nicht besser.

- Aufnahme und Speicherung durch
  - Videoüberwachung auf Straßen,
  - in Bahnhöfen, in Geschäften,
  - in öffentlichen Verkehrsmitteln
- Mautsysteme und automatische Kfz-Kennzeichenregistrierung in Parkhäusern und auf Straßen

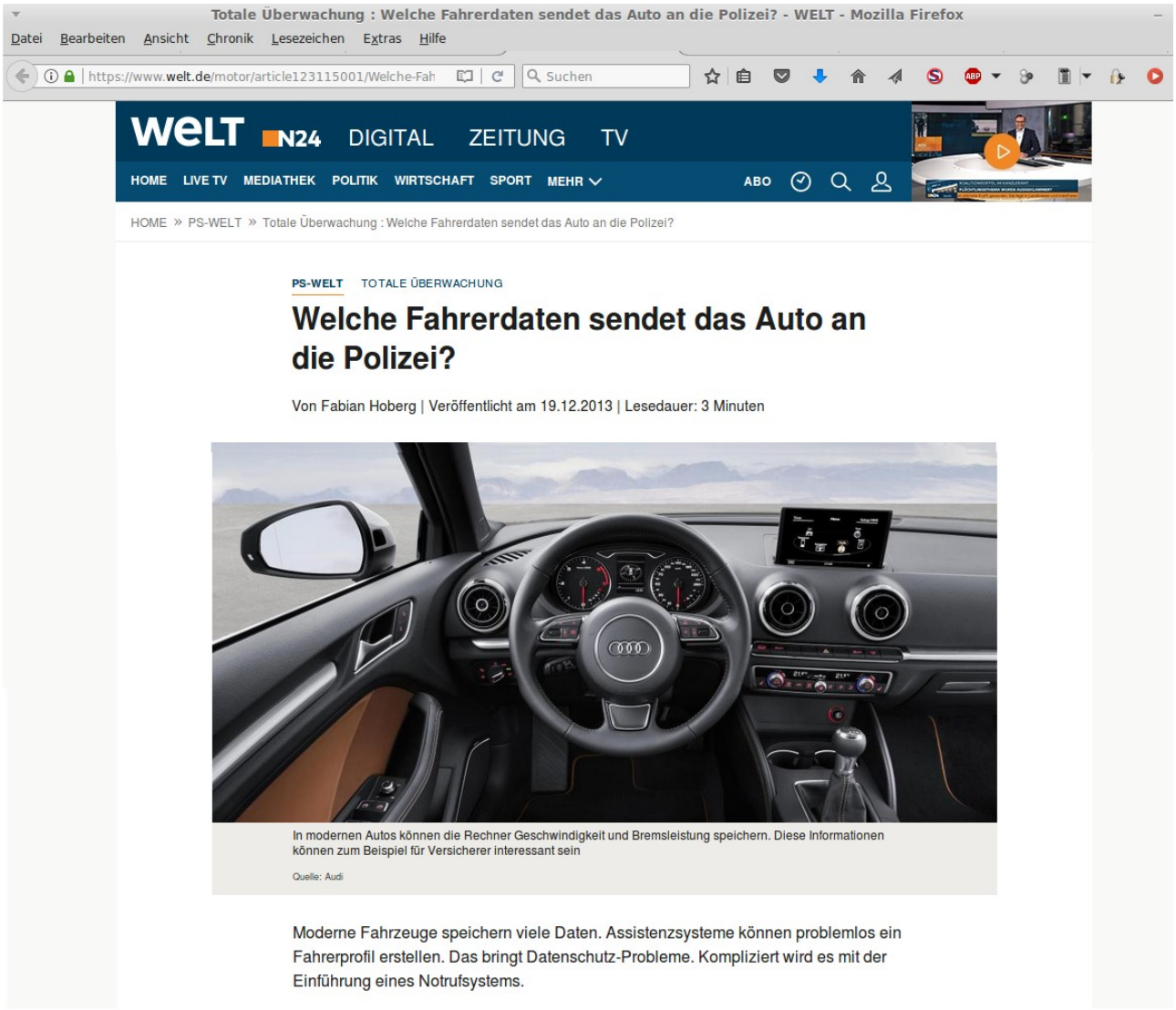
Die Videoüberwachung in London erfasst jeden Passanten ca. 70x pro Tag.

Die Maut-Systeme erfassen uns täglich auf den Straßen. Zur Zeit können wir noch davon ausgehen, dass nur LKW Daten langfristig gespeichert werden. Ab 2018 werden auch die Daten der PKWs für 5 Jahre gespeichert, weil wir ja nach 4 Jahren plötzlich widersprechen könnten, dass wir diese oder jene Straße damals genutzt hätten.

*Mhhm*? Eigentlich ist die PKW Maut doch, wie die GEZ eine "Steuer", die jeden Autofahrer trifft - wozu dann die angebliche Nachweispflicht über 5 Jahre?

Die private Kennzeichenerfassung nach irgendwelchen uns in der Regel unbekannten AGBs der Park- Kaufhäuser, denen wir mit dem Durchfahren der Schranke beim Einlass ahnungslos zustimmen, müsste eigentlich nach dem Bezahlen und Verlassen des Parkhauses beendet sein. Wo ist das Parkhaus, das die Daten in diesem Moment, dem Ende der Zweckbestimmung auch wirklich löscht?

Das eCall-System, die Vernetzung der Autos meldet dem Hersteller und dem Versicherer unser Fahrverhalten. In der Folge gibt es evtl. Tarifanpassungen und beim Unfall wird das Auto zum Zeugen gegen den Fahrer.




https://www.welt.de/motor/article123115001/Welche-Fahrerdaten-sendet-das-Auto-an-die-Polizei.html

Unsere Geodaten werden ohne Nachfrage getrackt, 41% der Handy-Apps nutzen unsere Geodaten, max. 10% würden sie für ihre Anwendung wirklich benötigen.
https://www.aktion-freiheitstattangst.org/de/articles/3100-20120831-geodaten-werden-ohne-nachfrage-getrackt.htm

# Industrie 4.0 und Smart Home

Alle reden vom IoT, dem Internet of Things. Die Geräte werden vernetzt und dürfen sich ungehindert miteinander unterhalten. Niemand weiß, wer welche Daten wohin sendet. Viele Beispiele dazu haben wir bereits in den vorigen Kapiteln gesehen.

Auch die Industrie rüstet ihre Fabriken mit Robotern und angeblich „intelligenter“ Steuerung aus. Das kann, wie tödliche Unfälle zeigen, durchaus gefährlich sein. Allein schon **wörtliche** Ausführung von Befehlen führt zu Mißverständnissen. https://www.aktion-freiheitstattangst.org/de/articles/5929-20170227-ki-nimmt-aussagen-von-menschen-woertlich.htm

Was ist im Kommen?

1. Smart Home mit Steuerung für
   - Heizung,
   - Wasser,
   - Licht,
   - Türen,
   - Fenster
   - Waschmaschine,
   - Kühlschrank,
   - Überwachung,
   - Strommessung durch Smart-Meter,

Gerade zum Smart-Meter gibt es viele Befürchtungen. Die Menschen werden gläsern, da man auf die Minute ganu weiß,

- wann sie nachHause kommen
- wie oft sie ihre Wäche waschen u.v. mehr.

Die Geräte, die auch von der Ferne gesteuert werden können, können die Stromzufuhr eines Konsumenten abschalten oder auf eine bestimmte Leistung begrenzen. Smart Metering könnte so für sozial Schwache zur Bedrohung werden. Hans Zeger von Arge Daten meint: "Es wäre denkbar, Arbeitslose oder Sozialhilfebezieher zu verpflichten, in lastarmen Zeiten zu kochen oder zu waschen, da sie als Arbeitslose ja ihre Zeit leichter einteilen könnten." https://www.aktion-freiheitstattangst.org/de/articles/1695-20101116-smart-meter-sorge-um-datenschutz.htm

2. Das Auto mit e-Call
   - meldet Standort
   - und Fahrverhalten
   - an Hersteller
   - und Versicherer
   -

Autofahrer sehen sich in ihrer Freiheit beschränkt, wenn die nicht beliebig „Gas geben“ dürfen, aber gegen die totale Überwachung ihrer Bewegungen sollen sie sich fügen?

3. In der Sicherheitsforschung ist man noch weiter

- eBorder und Smart-Border fertigen Geschäftsreisende schneller ab als den „Rest“. Die technikverliebten Ideen der EU Kommission bieten keine Vorteile bei der Grenzabfertigung aber massive Gefahren für die Privatsphäre und die Grundrechte der Menschen https://www.aktion-freiheitstattangst.org/de/articles/5532-20160430-forschung-zu-smart-border.htm
- mit Biosensoren ausgerüstete Schnüffelmaschine sollen die Grenzabfertigung verbessern https://www.aktion-freiheitstattangst.org/de/articles/4877-20150409-schnueffelmaschinen-fuer-eu-grenzen.htm

## Unternehmenswerte der Internetgiganten


Jeweils mit Unternehmenswert 2014/2015 in Milliarden $

Es gibt widersprüchliche Wertangaben und diese Werte schwanken. Man könnte stattdessen auch eine Hitliste der Gewinne angeben, die wohl aussagekräftiger wäre. In den Unternehmenswerten steckt kein produktiver Wert, es ist nur eine Spekulationsblase mit der weitere Unternehmen aufgekauft werden können. In der Regel werden  Startups gekauft und in das eigenen Unternehmen "eingemeindet" oder einfach „eingemottet“, das heißt sie verschwinden vom Markt je nach Belieben der Giganten. Damit lenken diese Unternehmen die Entwicklung und nicht, wie es in einer demokratischen Gesellschaft sein sollte die Politik und die Menschen.

# Zusammenfassung

Technische Systeme beobachten und spähen uns aus, sie verfolgen uns. Die Auswirkungen von Ausspähung, Beobachtung, Tracking:

- Kein Privatleben, keine Privatsphäre u. Intimsphäre das verletzt die Menschenrechte!
- Es wird ein unfreiwilliges, aufgezwungenes und automatisch-erstelltes, digitales Persönlichkeitsprofil NUR auf Grundlage von diversen Daten erstellt. Dies entspricht KEINER wirklichen Wahrnehmung unserer Person.
  - Fremdbestimmung,
  - Bevormundung,
  - Zwang und
  - Entmündigung,
  - Stalking,
  - Verfolgung
- Besondere Ausspähung der Verhaltensweise, Vorlieben, Interessen
- Die Schwerpunkte sind VERHALTEN und KONSUM!
- Wir werden unfreiwillig ausspioniert
- Nicht erwünschte Prognosen durch unsichtbare Datensammlung!

Unser Persönlichkeitsprofil wird NUR auf Grundlage von diesen diversen Daten erstellt. Es entspricht KEINER persönlichen Wahrnehmung.

- Zwang zur Nutzung = Entmündigung, denn Reichweiten und Konsequenzen der Technologie wird nicht in den AGB erklärt.
- Der User weiß davon nichts = Menschenrechtsverletzung und strafrechtsrelevant!
- Prognosen mit dieser unfreiwilligen Datensammlung führt zu Menschenrechtsproblemen, weil diese Prognose nicht erwünscht wurden!
- Scoring = Nachteile durch vorherigen Datenverlust, oder die Abgabe in Clouds, beim Einkaufen durch Payback
- Datenschutzverstoß durch erzwungene Einwilligung in Datenverarbeitung.

# Auswirkungen

Aus diesen genannten Fakten ergeben sich ernste Probleme:

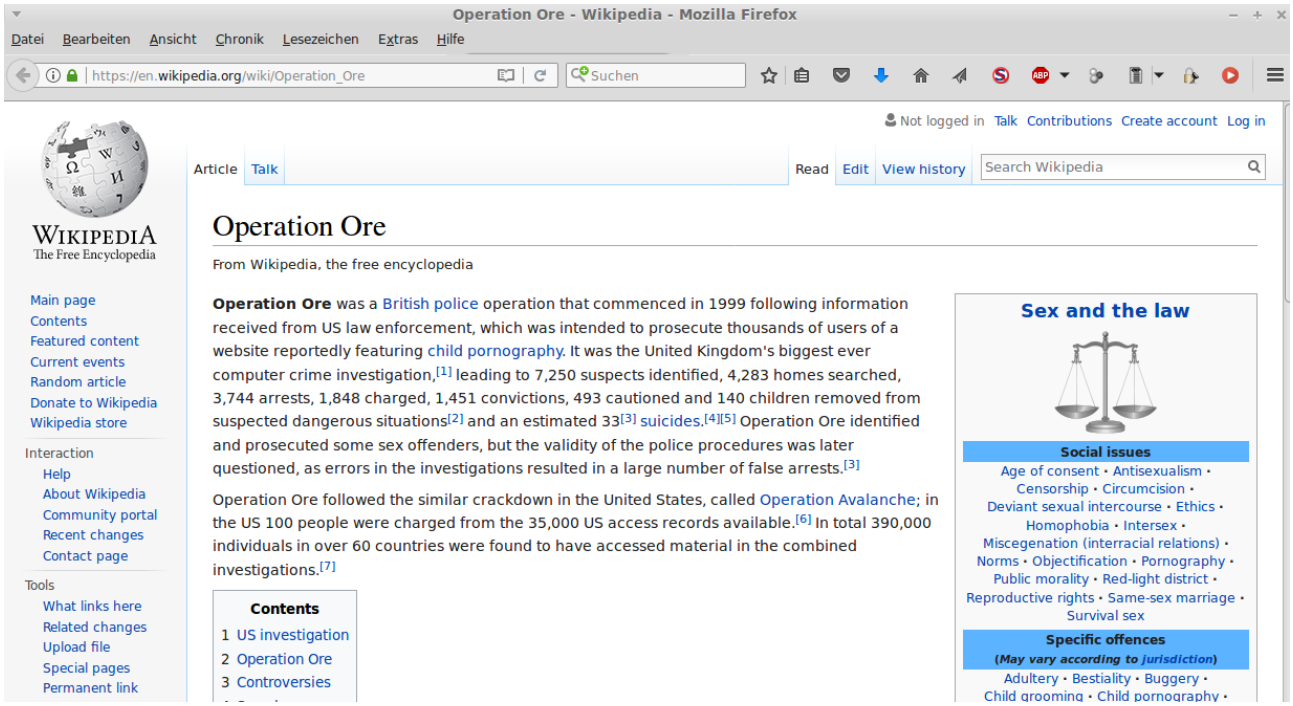
- False Positives (führt zur Umkehrung der Unschuldsvermutung und kann tödliche Folgen haben, s.u. )
- Stigmatisierung, Belästigung, Stresserhöhung und psychische Erkrankungen, wie Handysucht, Medienstress, ...
- **Abzocke**!!! Wenn wir z.B. an die durchschnittlichen 600MB/Tag denken oder das Smart Meter, das zu viel misst
- Verlust des freien Willens und Manipulation von Verhalten und Meinungen des Kunden und des Bürgers

**Vorsicht**: Die EU definiert z.Zt. "*Elektronische Personen*"

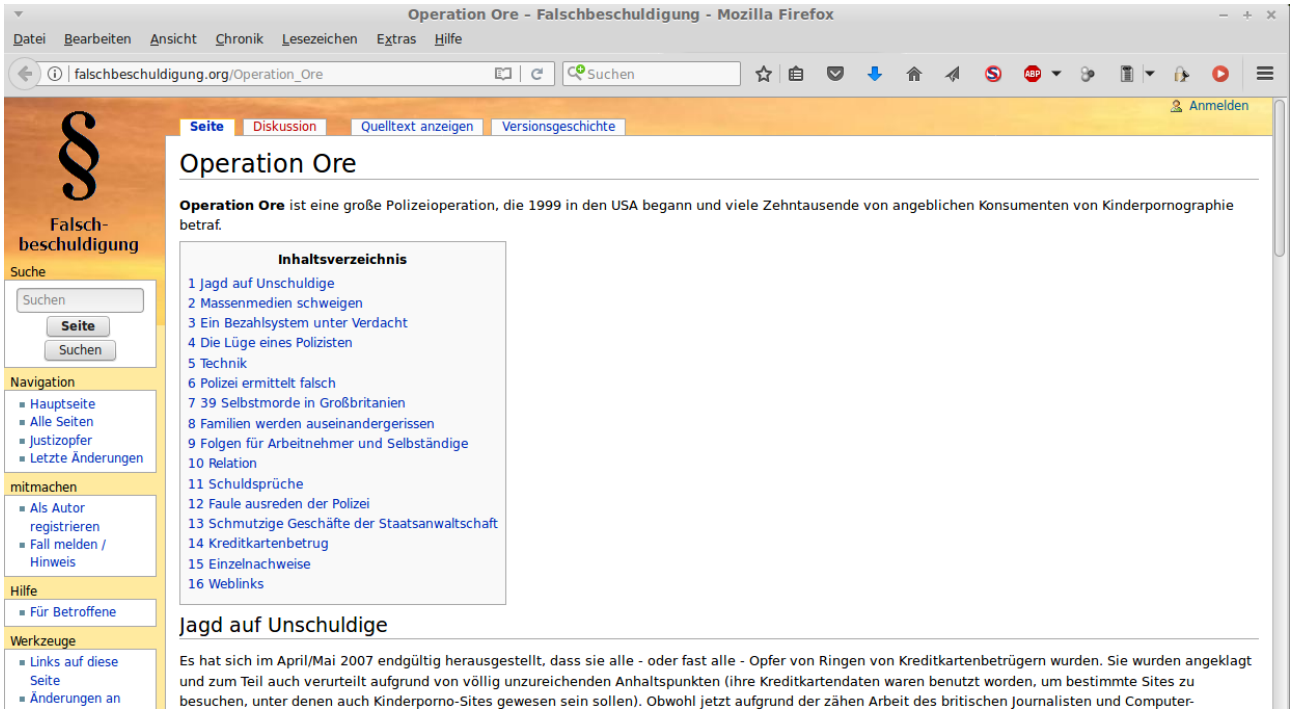
Vieles ist rechtlich und ethisch ungeklärt. Diese Dinge versucht die EU zu klären, in dem sie z.Zt. neben den Menschen und juristischen Personen nun elektronische Personen zu definieren versucht. Hier stehen für die Wirtschaft Haftungsfragen im Vordergrund. Die ethischen Probleme sollten aber nicht (wieder) vergessen werden.

## Beispiel für False Positives

Ein Beispiel für tödliche False Positives - für alle, die meinen, sie hätten nichts zu verbergen.




https://en.wikipedia.org/wiki/Operation_Ore
und http://falschbeschuldigung.org/Operation_Ore




Bei der Operation Ore hatte das FBI den britischen Behörden 1999 eine Liste übergeben, die sie aufgrund ihrer Zahlungen mit Kreditkarte für "Kunden" von Kinder-Pornoseiten hielten. Diese schlugen zu und

- untersuchten 7,250 suspects
- durchsuchten 4,283 homes searched
- verhafteten 3,744 arrests
- beschuldigten 1,848 charged
- verurteilten 1,451 convictions
- verwarnten 493 cautioned
- entzogen ihren Familien 140 children removed
- das führte zu Selbstmorden 33 suicides

Nach 6 Jahren steht fest, dass die Kreditkartennummern, bei Einkäufen in einem Grill-Shop in Florida genutzt wurden und dann von unbekannten Kriminellen auf (Kinder-) Pornoseiten genutzt wurden. 7000 Familien wurden zerstört, 140 Kinder aus Familien entfernt und über 30 Menschen haben sich deswegen das Leben genommen.

# Forderungen

Folgende Forderungen sind uns sofort eingefallen - es lassen sich sicher noch viele weitere aufstellen. Das wollen wir in der anschließenden Diskussion versuchen.

- Offenheit - Es darf keinen Zwang zu einem Gerät geben!
- z.B. bei Zugangssystem, Tickets, Geldverkehr
- Open Source – Software muss offen und kontrollierbar sein
- Vernetzung von personenbezogenen Daten muss grundsätzlich verboten sein (Zweckbindung), nur nach wirklich freiwilliger(!) Einwilligung
- Jedes Gerät im Haushalt und erst Recht am Körper muss einen echten(!) Aus-Schalter besitzen.
- Spracherkennung darf nur im Gerät nicht auf einem Server ausgeführt werden.
- Jedes Gerät überschreitet heute die Leistungsfähigkeit von Windows XP und kann so etwas ausführen.
- Für alle Kosten (z.B. beim Einwählen) und Schäden (False Positives und dessen Folgen) müssen die Hersteller haften!

# Was kann man zum eigenen Schutz selbst tun?

- Eigenverantwortung beim Umgang mit seinen Daten
- Verantwortung gegenüber Freunden und Anderen!
- Datensparsamkeit – Datenvermeidung
- Einhaltung der Zweckbindung

## Wie kann man das erreichen?

- Open Source statt Kommerz d.h.:
  - Mozilla Firefox, opera, ... statt M$ Explorer
  - Mozilla Thunderbird statt Outlook
  - Mail-Postfach z.B. bei Posteo.de, mailbox.org
  - statt bei Google, Yahoo, Microsoft, iCloud, web.de, gmx
- Gegen Malware und „neugierige Skripte“
  - schützende Plug-Ins im Browser verwenden,
  - z.B. noScript gegen Java, Ghostery, AdBlockPlus, ...
- Alternative Soziale Netzwerke nutzen
  - Diaspora, Telegram, Threema, Signal - statt Facebook & Twitter
- Firewall installieren
  - möglichst wenige Verbindungen erlauben, ca. 5-10 statt 65.000
- Verschlüsselung nutzen:
- beim Surfen https statt http,
- Tor Browser nutzen (der über verschiedene Hops geht und die eigene Identität verschleiern kann)
- Mail mit pgp signieren und verschlüsseln ( mit dem Plug-In Enigmail)
- Plug-In Mailvelope nutzen, wenn man Mails unbedingt im Browser lesen muss
- Bitmessage als Alternative zu normaler Mail verwenden (erzeugt keine Metadaten und kommt ohne Mail-Provider aus)
- eigene Daten verschlüsselt & getrennt von den Programmen speichern

# Diskussion

- Wusstet ihr das alles?
- War euch das alles oder das meiste bekannt?
- Weiß jede/r das?
- Was beobachtet ihr?
- Was bekommt ihr mit von den Leuten?
- Habt ihr schon mal Szenarien überlegt  die euch passieren könnten?

In unserem Web sind viele weitere Szenarien mit Datenpannen und -skandalen dokumentiert, einfach mal in der Suche Datenpanne oder Datenskandal eingeben.

# Linksammlung

Die Linksammlung umfasst beide Vorträge, also Überwachung durch "den Staat" und Überwachung durch Unternehmen und wird im Web von Zeit zu Zeit aktualisiert.

## Staatliche Überwachung

Bestandsdatenauskunft https://www.aktion-freiheitstattangst.org/de/articles/3534-20130415-bestandsdaten-ausser-kontrolle.htm
Bevölkerungsregister https://www.aktion-freiheitstattangst.org/de/articles/5856-20161226-auf-dem-weg-zu-einem-bevoelkerungsregister.htm
Biometrische Daten in Pass und ePerso, 2010 https://www.aktion-freiheitstattangst.org/de/articles/1203-biometrie.htm
Biometrie, Hack des ePerso https://www.aktion-freiheitstattangst.org/de/articles/1501-20100826-pressemitteilung-zum-hack-des-elektronischen-personalausweis.htm
BKA Gesetz, Nov. 2008 https://www.aktion-freiheitstattangst.org/de/articles/97-20090206-bka-gesetz.htm
Urteil zur Rasterfahndung
https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html
GTAZ https://www.aktion-freiheitstattangst.org/de/articles/1204-gtaz.htm

PNR: https://www.aktion-freiheitstattangst.org/de/articles/5304-20151209-keine-vorratsspeicherung-unserer-flugreisedaten.htm
PNR, Bruse Schneier http://www.schneier.com/essay-052.html
PNR, Edward Hasbrouck https://hasbrouck.org/articles/PNR.html
VDS: https://www.aktion-freiheitstattangst.org/de/articles/1329-20100514-gegen-die-eu-richtlinie-zur-vorratsdatenspeicherung.htm
https://www.aktion-freiheitstattangst.org/de/articles/1279-20100419-keine-neue-vorratsdatenspeicherung.htm
Steuer-ID https://www.aktion-freiheitstattangst.org/de/articles/1541-20100915-steuer-id-wird-zum-eindeutigen-schluessel.htm
Zensus 2011 https://www.aktion-freiheitstattangst.org/de/articles/1895-20110218-zensus-2011-schon-wieder-eine-volkszaehlung.htm

## EU-Forschung

https://www.aktion-freiheitstattangst.org/de/articles/659-20091009-interessante-zusammenfassung-zum-fp7-sicherheitsforschung-in-der-eu.htm
http://www.iq-wireless.com/en/r-and-d-service/amass-automatic-system-for-surveillance-of-the-

blue-border
http://imi-online.de/download/SL-JW-EUSicherheitsforschung-AusdruckFeb2010.pdf
http://www.iq-wireless.com/en/r-and-d-service/amass-automatic-system-for-surveillance-of-the-blue-border
https://stop-orwell2020.org
INDECT u. EU-Forschung https://www.aktion-freiheitstattangst.org/de/articles/1917-indect.htm

Erich Möchel der Staat als Krimineller https://media.ccc.de/v/fiffkon16-4003-cyber_der_staat_als_krimineller_/download
Liste Ueberwachungsgesetze https://www.aktion-freiheitstattangst.org/de/articles/1892-ueberwachungsgesetze.htm
BDSG Text: https://www.gesetze-im-internet.de/bdsg_1990/
Erläuterungen: https://en.wikipedia.org/wiki/Bundesdatenschutzgesetz
EU DS-GVO http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE
59. Konferenz der DSB vom 14./15. März 2000, Data Warehouse, Data Mining und Datenschutz
https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/59DSK-DataWarehouse_DataMiningUndDatenschutz.pdf
"Initiative Transparente Zivilgesellschaft" https://www.transparency.de/Initiative-Transparente-Zivilg.1612.0.html
Nichts zu verbergen http://www.nichts-zu-verbergen.de/

## Hacks

I love You https://de.wikipedia.org/wiki/ILOVEYOU
Stuxnet https://de.wikipedia.org/wiki/Stuxnet
Ellip.Curve Random Generator 2007 NIST Standard
http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115
Estland, April 2007 https://de.wikipedia.org/wiki/Internetangriffe_auf_Estland_2007
Litauen, Juli 2008 http://www.zdnet.com/article/300-lithuanian-sites-hacked-by-russian-hackers/
MHET, 2011 http://www.heise.de/newsticker/meldung/Geheimdienste-unterwandern-SIM-und-Kreditkarten-2555685.html
Shadow Brokers Leak, Sommer 2016
http://www.spiegel.de/netzwelt/web/shadow-brokers-cisco-und-fortinet-bestaetigen-sicherheitsluecken-a-1108277.html
http://thehackernews.com/2016/08/nsa-hack-russia-leak.html
http://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html
Manning Collateral Murder Video, 2010 http://www.zeit.de/1999/15/199915.36_bulk.xml

Snowden Veröffentlichungen, Juni 2013
https://www.aktion-freiheitstattangst.org/de/articles/3885-20131001-was-ist-neu-an-prism-tempora.htm

## Liste Datenpannen

https://www.aktion-freiheitstattangst.org/cgi-bin/searchart.pl?suche=panne&sel=meta
Gefahren durch Drohnen https://www.aktion-freiheitstattangst.org/de/articles/3310-20121215-drohnen-die-unsichtbare-gefahr.htm

## Arbeitnehmerdatenschutz

Historie - Arbeitnehmerdatenschutzgesetz https://www.aktion-freiheitstattangst.org/de/articles/903-historie-arbeitnehmerdatenschutzgesetz.htm

Gefeuert, weil sie App löschte https://www.aktion-freiheitstattangst.org/de/articles/4949-20150514-frau-gefeuert-weil-sie-ueberwachungs-app-loeschte.htm

## Verbraucherdatenschutz

eGK https://www.aktion-freiheitstattangst.org/de/articles/571-20090906-verbraucherdatenschutz.htm#egk
ELENA https://www.aktion-freiheitstattangst.org/de/articles/571-20090906-verbraucherdatenschutz.htm#elena
Gläserner Bürger https://www.aktion-freiheitstattangst.org/de/articles/571-20090906-verbraucherdatenschutz.htm#glas
Software-Ergonomie https://www.aktion-freiheitstattangst.org/de/articles/860-softwareergonomie.htm
„Nutzen“ von sozialen Netzwerken http://www.matthes-seitz-berlin.de/buch/facebook-gesellschaft.html
Steuerung durch soziale Netzwerke https://www.aktion-freiheitstattangst.org/de/articles/5839-20161212-online-manipulation-von-waehlern.htm
Smart-TV https://www.aktion-freiheitstattangst.org/de/articles/4777-20150210-vom-fernseher-zu-hause-ausspioniert.htm

## Informationsfreiheit

https://www.transparency.de/Initiative-Transparente-Zivilg.1612.0.html
Hate-Speech bei Zara Österreich
http://zara-training.at/