

Aber ich habe doch nichts zu verbergen!

Wege zu digitaler Mündigkeit



CryptoParty Graz

Zusammenfassung

Digitale Mündigkeit erfordert

1. ein **Grundverständnis von Strukturen und Prinzipien** hinter den Technologien der Digitalisierung (Codes, Algorithmen, Vernetzung, Möglichkeiten/Grenzen digitaler Kommunikation und künstlicher Intelligenz, etc.)
und
2. Befähigung die digitale Welt **verantwortungsbewusst mitzugestalten.**

3. Netzpolitischer Kongress, Berlin, 28.10.2016

Speed-Dating 5 – Digitale Mündigkeit

<https://www.gruene-bundestag.de/termin/3-netzpolischer-kongress-nk16-fuer-eine-ethik-der-digitalen-gesellschaft.html>





Seit den Aufdeckungen von Edward Snowden wissen wir, dass unsere digitale Kommunikation weltweit von Geheimdiensten überwacht wird.

- Manche wussten / vermuteten das auch schon vorher...

- vor 25 Jahren:

- z.B. Der Spiegel vom 20.2.1989

- "NSA: Amerikas großes Ohr"

- <http://www.spiegel.de/spiegel/print/d-13494509.html>

-

Echelon-System = globales elektronisches Aufklärungssystem

- Siehe z.B. Erich Moechel, www.fuzo-archiv.at/artikel/1652079v2



Totalüberwachung

- Warum wird überwacht ?
- Wer überwacht uns?
- Wo wird überwacht ?
- Was kann man/frau dagegen tun ?

Warum Überwachung ?

Staatliche Überwachung:

- Schutz vor Verbrechen und Terrorismus („Krieg gegen Terror“)

Warum Überwachung ?

Firmen als Überwacher:

- Wir wollen den KundInnen maßgeschneiderte, optimierte Produkte anbieten.
- Deshalb sollten wir die Wünsche der KundInnen genau kennen.
- Und deshalb sammeln wir
 - Interessensprofile
 - Tätigkeitsprofile
 - Persönlichkeitsprofile

Und:

- Prognosen über zukünftiges Verhalten können gemacht werden

Wer sammelt Daten ?

- Der Staat als Datensammler
- Geheimdienste als Datensammler
- Firmen als Datensammler
- Internet der Dinge
- Kriminelle
- Wir selber



Der Staat als Datensammler

Vorratsdatenspeicherung in Ö und EU gekippt, aber wieder in Diskussion

(keine präventive Wirkung gegen Terroranschläge)

- Melderegister der Gemeinden
- Finanzämter
- Versicherungen
- Grundbuch
- ...

Verknüpfung von online und offline Daten

Vorteile und Nachteile – die wichtigen Fälle sind so oft nicht greifbar



Geheimdienste als Datensammler

Geheimdienst NSA:

- NSA speichert **täglich 6 Milliarden Metadaten** (Emails, Telefonate, SMS)
- das entspricht etwa der Menge von 500 Millionen Büchern pro Tag
(Quelle: Heise-Newsticker 31.3.2014)
- aktuell anfallende Datenmenge im Internet:

$2,5 \cdot 10^{18}$ Bytes pro Tag = 2.500.000 Terabytes pro Tag

(Quelle: www1.logistik.fh-dortmund.de/IT-Sicherheit/IW_und_Ueberwachungsstaat.pdf)



Geheimdienste als Datensammler

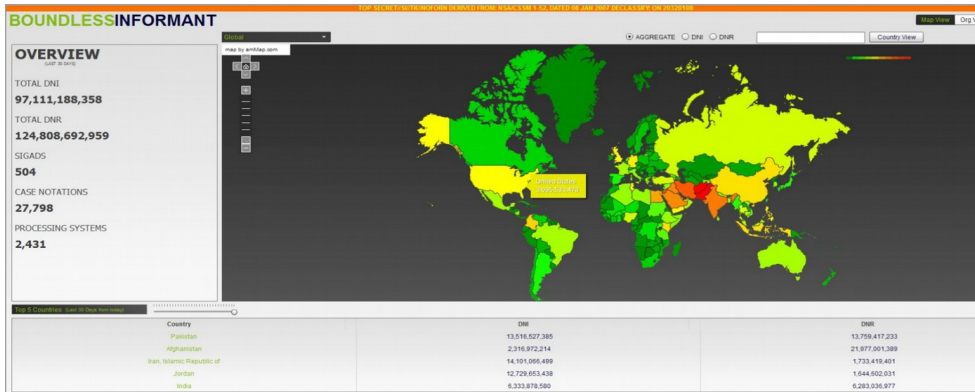
Britischer Geheimdienst GCHQ:

- Speicherte 2012 **täglich 50 Milliarden Metadaten** (Emails, Telefonate, SMS, Suchabfragen, Telefonstandorte, ...)
- Bis Jahresende 2012 war eine Verdopplung der Datenmenge geplant
- Die Datensammlung erfolgt bei grossen Webseiten
- Auswertung geschieht beinahe in Echtzeit
- Metadaten werden 1 – 6 Monate gespeichert, Kommunikationsinhalte 3 - 30 Tage lang
- Diese Daten stehen auch anderen Geheimdiensten zur Verfügung

Quelle: The Intercept, Der Standard 25.9.2015



Boundless Informant (eines der Überwachungsprogramme der NSA)



During a 30-day period, 97 billion internet data records (DNI) and 124 billion telephony data records (DNR) were collected.

Quelle: http://en.wikipedia.org/wiki/Boundless_Informant



PRISM (eines der Überwachungsprogramme der NSA)



Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple



What Will You Receive in Collection
(Surveillance and Stored Comms)?

It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:

Go PRISMFAA

URANIA 2016

TOP SECRET//SI//ORCON//NOFORN

CryptoParty.at/Graz



Firmen als Datensammler

Bei **Anmeldung im Internet**:

- Sind die Angabe von Name, Vorname, Straße, Ort, Postleitzahl und E-Mail- Adresse nötig !?!

Firmen benötigen **Kundendaten** für „Rechtsgeschäfte“
(z.B. Online-Einkauf)

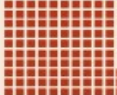
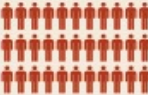
- Wohin sonst sollen sie die Ware schicken?
- Woher sonst sollen sie ihr Geld bekommen?

Daten-Sammelwut :

- bei vielen Anmeldungen würde nur ein Bruchteil der abgefragten Informationen genügen.



Die Macht der Internetkonzerne

	Umsatz ¹ 2013	Gewinn ¹ 2013	Beschäftigte 2013
 Apple	 191,9	 41,6	 80.300
 amazon	 83,7	 0,3	 117.300
 Google	 67,2	 14,5	 47.756
 Facebook	 8,8	 1,7	 6.337
Alle 20 ATX-Konzerne	 113,1	 5,1	 334.450

Quelle: „Vorstandsvergütung in ATX-Unternehmen“ AK (2014);
 U.S. Securities and Exchange Commission; Statista; AK/ÖGB-Darstellung.

¹ Mrd. Euro

Firmen als Datensammler

Daten sammeln als Geschäftsmodell

Wenn der Dienst gratis ist, sind wir die Waren
(aber auch, wenn er nicht gratis ist...)



Apps: Spione in der Hosentasche

Top-100-Apps



Android



iOS

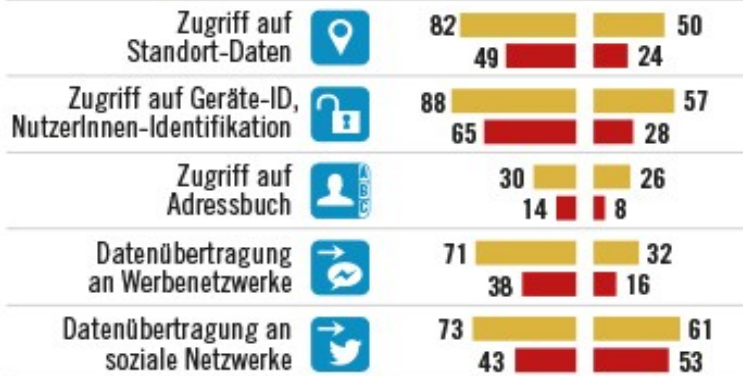
Anteil in %



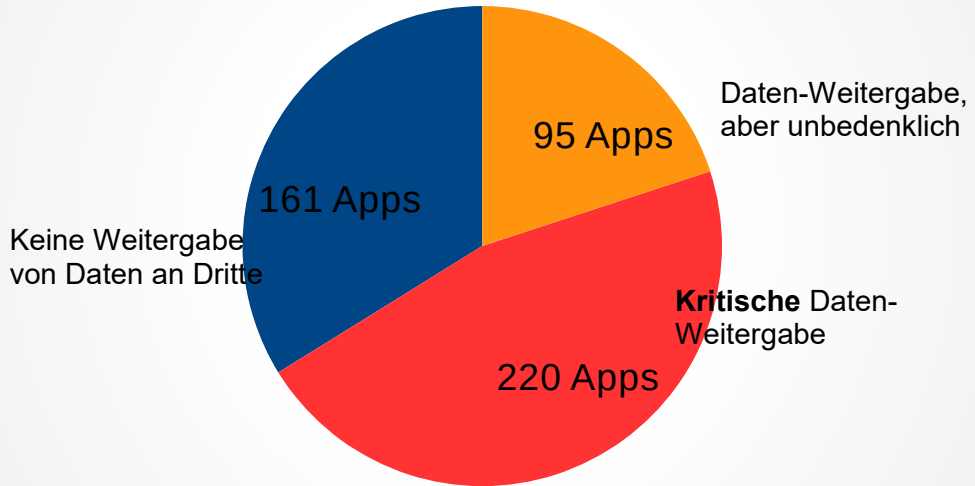
kostenlos



kostenpflichtig



Datenversand an Werbe- und Analysenetzwerke



Quelle: Mediatest Digital,
c't Überwachung 2015

Datenweitergabe von Handy-Apps

- Untersuchung von Stiftung Warentest 06/2012
- 63 Apps wurden untersucht
- Ergebnis:
 - 9 Apps: sehr kritisch
 - 28 Apps: kritisch
 - 32 Apps: verlangen Geräte-ID, davon 18 mit Nutzungsprofil
- Alles, ohne den Nutzer zu informieren !

Name und Version ¹⁾	Betriebs- system	Preis in Euro ca.	Im Datenstrom identifiziert	test-Kommentar
Alltagshelfer				
 Barcode Scanner V. 4.0				
 Brutto Netto Gehalt Rechner V. 1.8				
 Free App Magic V. 1.4				
 Mobile Metronom V. 1.2.4				
 QR Droid V. 4.1.2				
 Torch V. 1.1.0				
Auto und Reise				
 Navigon Mobile Navigator Europa V. 2.0.2				
 Nokia Navigation V. 1.0.0.1				
 Skobler GPS Navigation 2 V. 4.1				
 Stau Mobil V. 2.0				
Einkaufen				
 Amazon Mobil V. 1.8.1				
Ernährung				
 chefkoch.de V. 1.0				

Name und Version ¹⁾	Betriebs- system	Preis in Euro ca.	Im Datenstrom identifiziert	test-Kommentar
Freizeit				
 iKamasutra lite V. 5.0.1	iOS	0,00	●	Sendet Gerätekennung und Benutzungsstatistik an flurry. Kommuniziert mit Servern von Fremdfirmen wie mobidix und smaato.
 Smart Runner V. 2.5	iOS	0,00	●	Sendet Gerätekennung und Benutzungsstatistik an flurry.
Lokales				
 Das Örtliche V. 1.14	Android	0,00	●	Überträgt Gerätekennung und Standortdaten an Server von Fremdfirma. Fordert Zugriff auf Kontaktdaten.
 Fahrrinfo Berlin Brandenburg V. 2.8.3	iOS	0,00	●	Sendet Gerätekennung, allerdings nur an den eigenen Server.
 KlickTel Telefonbuch V. 5.2	Android	0,00	●	Sendet Gerätekennung und Benutzungsstatistik, allerdings nur an den eigenen Server.
 KlickTel Telefonbuch V. 5.2	iOS	0,00	●	Standortdaten gehen auch an dealorio. Benutzungsstatistik geht an eigenen Server. Sendet Gerätekennung an smaato.
 meinsStadt V. 3.2.1	iOS	0,00	●	Sendet Gerätekennung. Kommuniziert mit Servern von Fremdfirmen.
 Weather Live V. 1.4	iOS	0,79	●	Benutzungsstatistik und Gerätekennung gehen an flurry. Kommuniziert mit Servern von Fremdfirma.
 Weather XXL lite V. 1.4.3	iOS	0,00	●	Sendet Gerätekennung. Kommuniziert mit Servern von Fremdfirmen.
Medien, Nachrichten				
 MacWelt V. 4.0	iOS	0,00	●	Sendet Gerätekennung, allerdings nur an eigenen Server.
 N-TV iPhone edition V. 1.6.1	iOS	0,00	●	Sendet Gerätekennung. Kommuniziert mit Servern von Fremdfirmen wie doubleclick.
 Sport1 V. 5.1.2	iOS	0,00	●	Sendet Gerätekennung. Kommuniziert mit Servern von Fremdfirmen.
Spiele				
 Angry Birds V. 2.0.0	Android	0,00	●	Protokolliert und sendet kompletten Spielablauf sowie Gerätekennung an flurry.
 Bubble Blast 2 V. 2.1.3	iOS	0,00	●	Sendet Gerätekennung unter anderem an admob. Überträgt Mobilfunkanbieter. Kommuniziert mit Servern von Fremdfirmen.
 Solitaire V. 1.2	iOS	0,00	●	Sendet Gerätekennung und Benutzungsstatistik an flurry.
 Sudoku V. 1.0.2	iOS	0,00	●	Sendet Gerätekennung an admob. Kommuniziert mit Servern von Fremdfirmen.

Reihenfolge nach Alphabet. ● = Ja. 1) Laut Anbieter der App-Stores zum Teil neue Versionen der Apps verfügbar. 2) Angaben zu Nutzungsdauer und -umfang.

Einige Datensammler & Datenhändler

DISPLAY LUMAscape



 http://www.heise.de/tp/bild/43/43207/43207_1.html

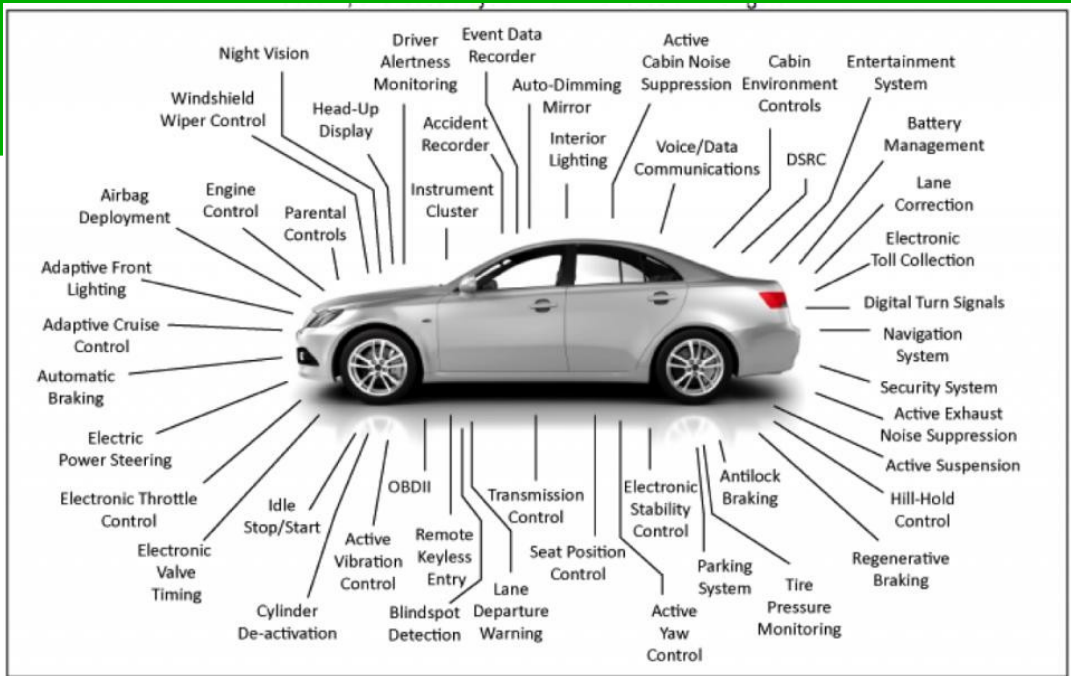
LJMA Partners LLC 2014



Internet der Dinge

- Smartmeter – Stromverbrauch
- Wasserverbrauch
- Kühlschränke: kennen unser Ernährungsverhalten
- Autoversicherung: Sensoren im Auto erfassen Fahrverhalten
- Smart Cities
- Smarte Autos





<http://www.forbes.com/sites/tomcoughlin/2016/07/20/the-memory-of-cars/#47e3de4c5fd7>

10.11.2016

URANIA 2016

CryptoParty.at/Graz



Der Gesamt-Score besteht aus vier Unter-Scores, der Ausgangswert ist jeweils 100.

Gesamt-Score

Berechnungsregeln

40 % Fahrweise

- Starkes Beschleunigen* oder starkes Bremsen** führt zu einem „Ereignis“
- Die ersten beiden „Ereignisse“ führen zu jeweils 20 Punkten Abzug, weitere „Ereignisse“ zu jeweils 10 Punkten Abzug (auf 100 km umgerechnet)

30 % Geschwindigkeit

- „Ereignis“: Überschreitung der vorgegebenen Geschwindigkeit um 20 %, mindestens 10 km/h
- „Ereignis“ aber erst dann, wenn zwei Messungen hintereinander eine Überschreitung feststellen (also innerhalb 30 Sekunden), damit Ausschließen kurzzeitiger Überschreitungen
- Jeder „km zu schnell“ auf 100 km führt zu 20 Punkten Abzug
- Beispiel: 2 „km zu schnell“ auf einer 200-km-Fahrt führen zu einem Abzug von 20 Punkten und damit zu einem Unter-Score für Geschwindigkeit von 80

20 % Nachtfahrt

- Nachtfahrten sind Fahrten zwischen 23 Uhr und 5 Uhr
- Der Anteil der Nachtfahrten in km an der Zahl der gefahrenen Gesamt-km definiert den Abschlag bei diesem Score
- Beispiel: Eine Fahrt von 200 km, davon 20 km nach 23 Uhr bedeuten einen Abschlag von 10 und damit einen Unter-Score für Nachtfahrten von 90

10 % Stadtfahrt

- Stadtfahrten sind definiert als Fahrten in Gebieten mit Geschwindigkeitsbegrenzung von 50 km/h oder weniger
- Score-Berechnung wie bei Nachtfahrten

* mehr als 0,235 g = 2,3 m/s² ** mehr als 0,286 g = 2,8 m/s²

Kriminelle

- Kriminelle, die an unsere Kennwörter und Konten heranwollen oder mittels Erpressung Geld fordern

z.b.

- Verschlüsselungs-Trojaner
- Phishing-Mails
- Nigeria-Connection

Wir

Wir selber „liefern“ viele Daten:

- durch Postings in Sozialen Netzen
- durch Verwendung von
 - Kreditkarten
 - Kundenkarten
 - Life-Tracker



2006

[https://en.wikipedia.org/wiki/You_\(Time_Person_of_the_Year\)](https://en.wikipedia.org/wiki/You_(Time_Person_of_the_Year))

Datenprofile

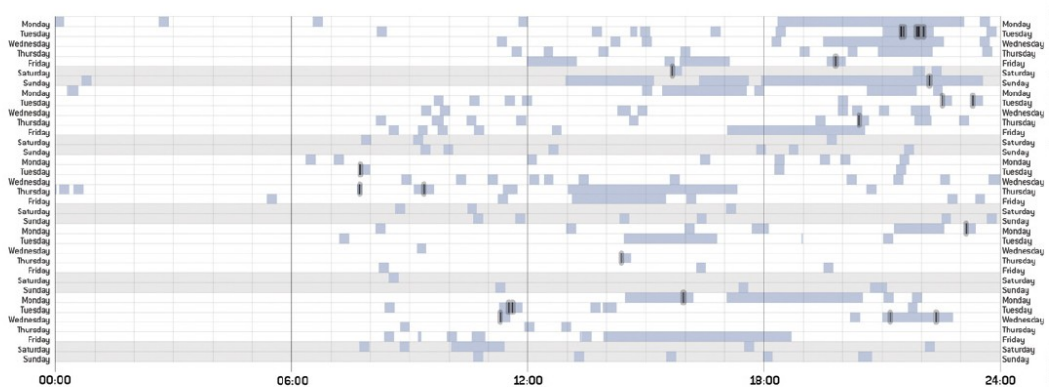
- Aus den gesammelten Daten werden **Profile** der Internet-Benutzer erstellt
 - „digitaler Schatten“
 - „digitales Ich“
- Diese **Datenprofile** mit tausenden Persönlichkeitsmerkmalen werden an Firmen verkauft (Versicherungen, Arbeitgeber, Internet-Werber ...)

Social Graph – Max Schrems



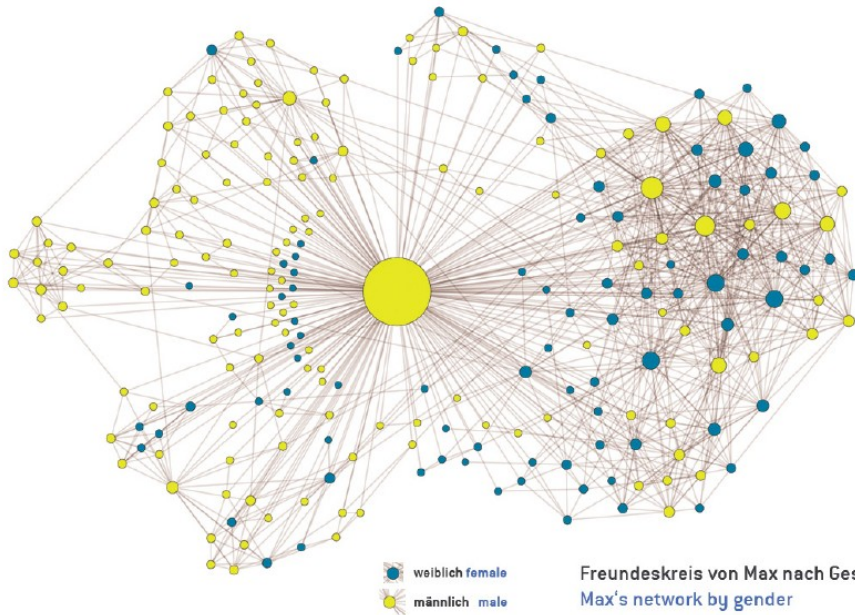
Schlagworte aus Max' Nachrichten
Tags from Max's messages

Social Graph – Max Schrems



Beispiel: Wann war Max eingeloggt und wann schrieb er Nachrichten (schwarze Linien)

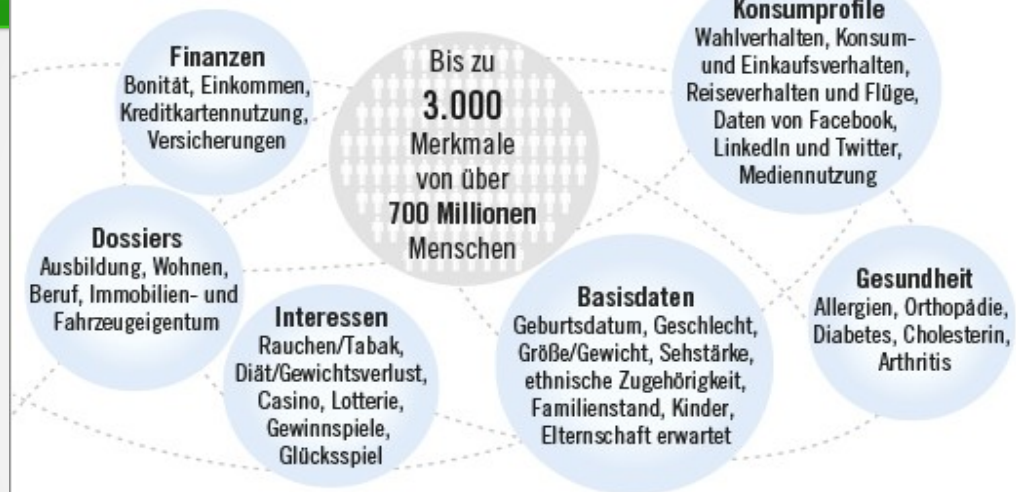
Social Graph – Max Schrems



Social Graph – Max Schrems



Das Datenangebot des US-Datenhändlers Acxiom



ACXIOM

Dossiers

Ausbildung,
Wohnen, Beruf,
Immobilien-
und Fahrzeug-
eigentum

Finanzen

Bonität,
Einkommen,
Versicherungen
Kreditkarten-
nutzung

Gesundheit

Allergien,
Orthopädie,
Diabetes,
Cholesterin,
Arthritis

Interessen

Rauchen/Tabak,
Diät/Gewichtsverlust,
Casino, Lotterie,
Gewinnspiele,
Glücksspiel

Konsumprofile

Wahlverhalten,
Konsum- und Einkaufs-
verhalten, Mediennutzung,
Reiseverhalten und Flüge,
Daten von Facebook,
LinkedIn und Twitter

Bis zu **3.000**

Merkmale

über

700 MIO

Menschen

Basisdaten

Geburtsdatum,
Geschlecht, Sehstärke,
Körpergröße/-gewicht,
ethnische Zugehörigkeit,
Familienstand, Kinder,
Elternschaft erwartet

CC BY-SA 3.0 Cracked Labs

Beispiele aus dem "Consumer Data Products Catalog" des US-Unternehmens
Acxiom, das bis zu 3.000 einzelne Eigenschaften über 700 Millionen Menschen anbietet

Beispiele aus dem Consumer Data Products Catalog von Acxiom

<https://www.hashdoc.com/documents/8135/data-products-catalog>

CRYPTO-
PARTY

Persönliche Daten sind bares Geld wert

	Adressen	Beschreibung	Preis pro T.
Die Zeit	55.900	Shopkäufer und Buchserienkäufer	€ 210,00
RTL Club	510.000	aktive Kunden	€ 180,00
Elderly & Disabled	110.000	Spender	€ 175,00
Tag des Herrn	52.400	Abonnenten katholische Wochenzeitung	€ 170,00
Lehrer	246.100	mit Privatanschrift	€ 170,00
Lehrer	367.700	mit Schulanschrift	€ 170,00
Die Zeit	374.000	aktuelle Leser und ehem. Abonnenten	€ 160,00
Passive Ältere	3.051.100	Adressen gesamt	€ 155,00
Versa Distanzhandel	55.700	aktive Käufer 0-6 Monate (Beate Uhse)	€ 150,00
Gewinnspielteilnehmer	215.500	Gewinnspielteiln. Drogerieartikel	€ 150,00
Große Tageszeitung	2.155.000	Werbedatei einer großen Tageszeitung	€ 110,00

CC BY-SA 3.0 Cracked Labs

Beispiele für von AZ Direkt/Bertelsmann im Online-Katalog angebotene Adressen (11/2014)

Was kann man mit den Datenprofilen machen ?



Quelle: www.crackedlabs.org; AK/ÖGB-Darstellung.

Arbeit&Wirtschaft 7/2015

ÖGB-VERLAG/APA-AUFTRAGSGRAFIK

Techniken zum Tracking des Surfverhaltens

- Cookies
- Flash-Cookies
- Webbugs
- Werbung, Like-Buttons
- EverCookie-Techniken
- Browser-Fingerprinting
- Keystroke Biometrics

Getrackt wird auch bei

- Emails, Newslettern
 - z.b. mit Webbugs (1x1-Bildchen), die nachgeladen werden müssen
 - Links führen über Trackservice
- Tracking von Dokumenten
 - Teile des Dokuments werden nachgeladen und tracken den User

Cookies

- Die am meisten angewendete Technik, um Internet-Nutzer zu beobachten
- Empirische Studien:
 - 160 Trackingdienste, die 40 % des Surfverhaltens erfassen
 - z.B.
 - Google Analytics, Chartbeat.com, AudienceScience.com, WebTrek, Yahoo! Web Analytics: täuschen vor First-Party Content zu sein
-

- **Flash-Cookies:**

- werden verwendet, um gelöschte Tracking-Cookies wiederherzustellen
- Sind nicht blockierbar

- **Webbugs** (od. Web-Beacons):

- sind 1x1-Pixel große transparente Bilder
- sind für den Nutzer unsichtbar
- werden von speziellem Server geladen und hinterlassen dort Spuren (Log-Datei)
- können Cookies setzen

- **Werbung und Like Buttons:**
 - werden einerseits wie Webbugs verwendet
 - mit Klicks auf Werbung oder "Like Buttons" verrät man mehr private Informationen, als man eigentlich veröffentlichen möchte
 - Werbung kann auch ein Einfallstor für Schadsoftware sein
- **EverCookie Techniken:**
 - nutzen moderne HTML5 Techniken wie DomStorage, ETags aus dem Cache u.a. als Ersatz für Cookies, um den Surfer zu markieren

Persönlichkeitseigenschaften aus Facebook-Likes

Eigenschaft	Zuverlässigkeit der Prognose	Was wurde genau untersucht?
Ethnischer Hintergrund	95%	Kaukasisch oder Afro-Amerikanisch?
Geschlecht	93%	Männlich oder weiblich?
Sexuelle Orientierung I	88%	Schul?
Politische Einstellung	85%	Liberal oder konservativ?
Religion	82%	Christlich oder muslimisch?
Sexuelle Orientierung II	75%	Lesbisch?
Nikotinkonsum	73%	Raucher/Raucherin?
Alkoholkonsum	70%	Trinkt Alkohol?
Beziehung	67%	Single oder in einer Beziehung?
Drogenkonsum	65%	Konsumiert Drogen?
Trennungskind	60%	Eltern im Alter von 21 getrennt?

Erfolgsraten bei der Prognose von Persönlichkeitseigenschaften aus Facebook-Likes. Quelle: Kosinski et al, 2013

CC BY-SA 3.0 Cracked Labs

Quelle: Kosinski et al, 2013
<http://www.pnas.org/content/110/15/5802>

Browser Fingerprinting

verschiedene **Merkmale des Browsers** werden zur Erkennung benutzt wie z.B.

- Browserversion, Browser-Plugins
- installierte Schriftarten, Reihenfolge der Installation
- Bildschirmgröße,
- bevorzugte Sprachen
- Informationen über die eingesetzte Hardware
- ...

Daraus wird ein „**Fingerprint**“ berechnet

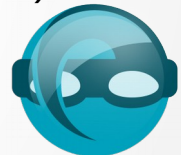
Dieser Fingerprint ist für viele Surfer eindeutig

- Projekt **Panopticlick** der EFF.org : mehr als 80% der Surfer sind damit eindeutig erkennbar
- <https://panopticlick.eff.org/>

Browser Fingerprinting - Gegenmassnahmen

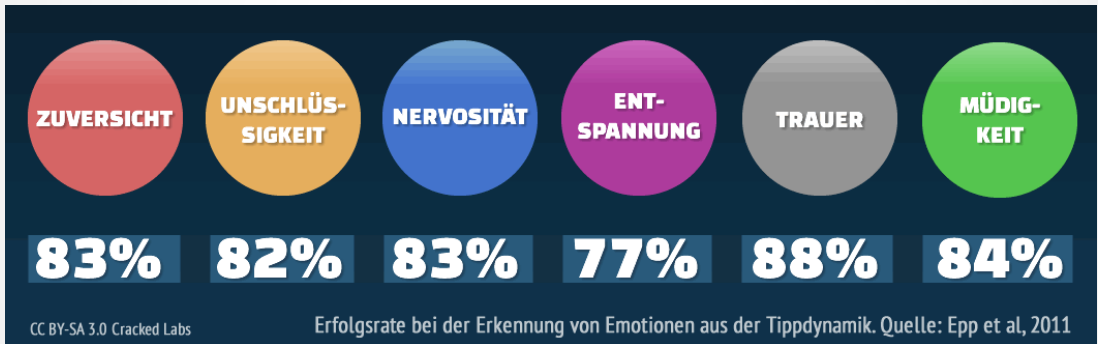
Was kann man gegen Browser Fingerprinting machen?

- Tor-Browser benutzen
- JavaScript ausschalten (z.B. mit dem Plugin NoScript“)
- Einen sehr gängigen Web-Browser benutzen
- Die Privacy-Machine benutzen (made in Graz!)



Keystroke Biometrics

- verwendet das Schreibverhalten der Nutzer auf der Tastatur als Identifizierungsmerkmal



Erfolgsrate bei der automatisierten Erkennung von Emotionen aus der Tastenanschlags-Dynamik.
Quelle: Epp et al, 2011 <http://hci.usask.ca/uploads/203-p715-epp.pdf>

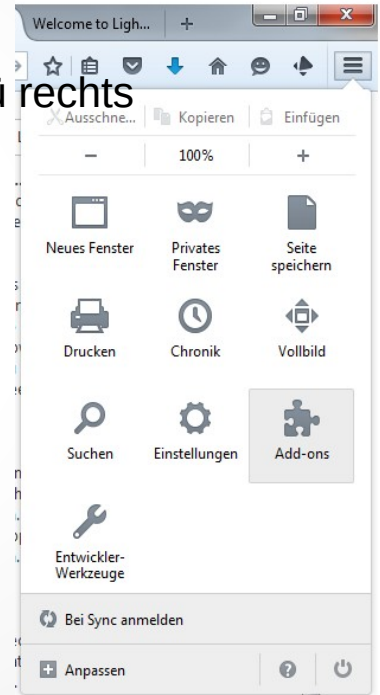
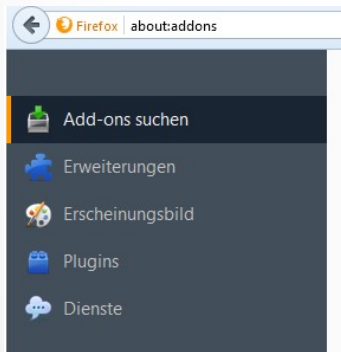
Keystroke Biometrics in Windows 10

- Das Schreibverhalten der Anwender wird im Hintergrund durch das Betriebssystem automatisch analysiert
- die erstellten biometrischen Profile werden an die Firma BehavioSec gesendet
- BehavioSec kooperiert mit der DARPA und Microsoft
- Laut Eigenwerbung kann BehavioSec **99% der Nutzer korrekt erkennen.**
- Die dabei entstehende umfangreiche Sammlung der biometrischen Profile kann zukünftig zum Tracking und zur Deanonymisierung genutzt werden.

- **Privacy-Handbuch, Tracking-Techniken**
- https://privacy-handbuch.de/handbuch_13.htm
- **Studie von Wolfie Christl: Kommerzielle digitale Überwachung im Alltag**
- <http://crackedlabs.org/studie-kommerzielle-ueberwachung>
-
-
- <https://myshadow.org/trackography>
- <https://myshadow.org/tracking-data-traces>
- <https://trackography.org/>
-
- **Der gläserne Nutzer - Datenspuren im Internet**
- **Vortrag von Helmut Eiermann, 2012**
- https://www.datenschutz.rlp.de/downloads/vortraege/20120615_-_Eiermann_-_Frankfurt_-_Datenspuren.pdf

Add-ons in Firefox installieren

- Add-ons in Firefox werden im Menü rechts aufgerufen:
- Und links oben kann man nach einzelnen Add-ons suchen :



Empfohlene Plugins für Webbrowser

- **Schutz gegen Web-Tracking mit Privacy-Badger :**
- <https://www.eff.org/privacybadger>
- **Visualisierung von Web-Tracking mit Lightbeam** für Firefox:
<https://de.wikipedia.org/wiki/Lightbeam>
- Werbefblocker **uBlock Origin**:
- https://en.wikipedia.org/wiki/UBlock_Origin
- **Automatischer Aufruf von verschüsselter Datenübertragung:**
- **HTTPS Everywhere:** <https://www.eff.org/https-everywhere>

Visualisierung von Web-Tracking

mit Lightbeam für den Webbrowser Firefox:

- <https://www.mozilla.org/en-US/lightbeam/>
- <https://de.wikipedia.org/wiki/Lightbeam>

