

Digitale Selbstverteidigung

Gefahren aus dem Internet

23.11.2017



Letzte Woche:

- Wer überwacht uns ?
- Wo & wie werden Daten erfasst ?

Heute:

- Profilbildung, Predictive Analysis
- Gegenmassnahmen



Ein paar aktuelle Nachrichten-Meldungen
aus dieser Woche ...



Uber verschwieg Diebstahl der Daten von über 50 Millionen Kunden

21. November 2017, 23:55



87 POSTINGS

100.000 Dollar Schweigegeld an Hacker gezahlt – Keine Kreditkartendaten oder Informationen gestohlen

Dem Fahrdienstvermittler Uber sind bereits vor gut einem Jahr Daten von rund 50 Millionen Fahrgästen **gestohlen worden**. Das skandalgeschüttelte Start-up verschwieg aber den Vorfall und informierte die Öffentlichkeit erst am Dienstag. Es gehe um Namen, E-Mail-Adressen und Telefonnummern von Nutzern rund um die Welt, erklärte Uber.

Außerdem hätten sich die Angreifer auch Zugriff auf Daten von etwa sieben Millionen Uber-Fahrern verschafft. Es seien nach bisherigen Erkenntnissen aber keine Kreditkartendaten oder Informationen zu Fahrten gestohlen



Datendiebstahl

Der Kunde ist dem IT-Unternehmen „ausgeliefert“, wenn es ihm seine Daten anvertraut

Beispiele:

- **LinkedIn:** 117 Millionen Passwörter im Netz verfügbar
- **Yahoo:** Daten zu 3 Milliarden (!) Konten entwendet
- **Uber:** 50 Millionen Kundendaten gestohlen

Gefährlich ist meist die Verknüpfung von Einzeldaten



Hunderte der beliebtesten Webseiten überwachen jede Texteingabe

21. November 2017, 09:25



Studie warnt vor problematischen Skripten – Kreditkartendaten und Passwörter an Dritte weitergereicht

Wer eine Webseite besucht, liefert dem jeweiligen Betreiber damit im Normalfall auch jede Menge Daten. Doch in welchem Ausmaß solch ein Tracking erfolgt, variiert dabei stark. Eine aktuelle Studie zeigt nun, wie weit dabei einzelne Seiten gehen – und wie problematisch dieses Verhalten ist.



Webseiten-Überwachung

„Session Replay“-Skripte:

Aufgezeichnet werden kann während des Web-Surfens:

- Mausbewegungen
- Scrollverhalten
- Jegliche Tastatureingaben auf einer Webseite

In Echtzeit !

z.B. Passwörter, Kreditkarteninformationen

Diese Daten können auch von Dritt-Anbietern genutzt werden

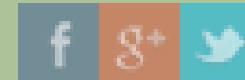
Betroffen sind viele Webseiten grosser Unternehmen



Google sammelte im Geheimen Ortsdaten von Android-Nutzern

ANDREAS PROSCHOFSKY

22. November 2017, 09:16



10 POSTINGS

Selbst wenn Location Services deaktiviert waren – Unternehmen spricht von Versehen, Daten seien nie verwendet worden

Wer ein Smartphone verwendet, liefert damit dem jeweiligen Anbieter jede Menge Informationen über die eigenen Aktivitäten. Dem sind sich mittlerweile wohl die meisten User bewusst, oder haben dem Ganzen zumindest mittels mehr oder weniger unverständlichen Nutzungsbedingungen zugestimmt. Doch manchmal sammeln die Unternehmen noch wesentlich mehr Daten als die Nutzer erwarten dürfen – und genau dabei wurde nun eine der Größen der Branche erwischt.



Android sammelt Standortdaten trotz Widerspruch des Nutzers

21.11.2017

<https://www.heise.de/newsticker/meldung/Android-sammelt-Standortdaten-trotz-Widerspruch-des-Nutzers-3896047.html>

Trotz Deaktivierung: Android schickt Standort an Google

<https://futurezone.at/digital-life/trotz-deaktivierung-android-schickt-standort-an-google/299.018.328>



Google collects Android users' locations even when location services are disabled

21.11.2017

<https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/>



Die amerikanische News-Seite Quartz entdeckte, dass jedes Android-Handy Standortdaten an Google ermittelt.

Auch, wenn die Standortdienste abgeschaltet sind, ohne Nutzung einer App oder einer eingelegten SIM-Karte.

Gesammelt werden die Kennungen der Mobilfunk-Türme in der Nähe des Geräts.



Google gab zu, dass diese Datenübermittlung
seit Jänner 2017 besteht und kündigte eine
Beendigung in 2 Wochen an.

Laut Google wurden die übermittelten Daten nicht
gespeichert oder genutzt ?!?

Grund für die Datenübermittlung:
Push-Nachrichten verbessern ?!?



20170624T200834Z-192.168.89.104,44455-64.233.186.188,443.log

```

gms-10.9.00-000mcs.android.com3792908341944979238"3792908341944979238*9059819305718439
CONOK0B
os_ver
android-26B
u:f0B
network0n202B

network0ff549j
!pxÄàëöst0P_6Ia6koYgN2FymWCIBPG5w2ntgI¢
CDMA,18,3,297®<Óß<Ö+≤†Q≤¿
»
# /

```

API Sandbox

LocationAPI

Geocoding

Maps

Timezone

User Reports

User reports

Device reports

Bulk Requests

Account details

Support

LocationAPI will return a location if you provide Cell Towers, WiFi APs near a device. View the [API documentation](#) here.

Request: 1 Cell - CDMA

```

1 {
2   "token": " ",
3   "radio": "cdma",
4   "mnc": 18,
5   "cells": [{
6     "lac": 3,
7     "cid": 297
8   }],
9   "address": 1
10 }

```

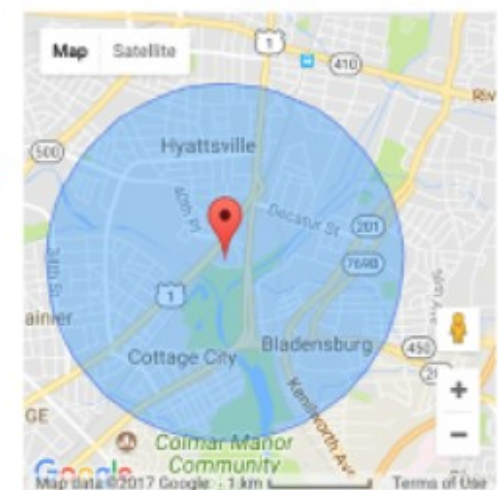
Response:

```

1 {
2   "status": "ok",
3   "balance": 99,
4   "lat": 38.94612,
5   "lon": -76.943791,
6   "accuracy": 1660,
7   "address": "Charles Armentr
8 }

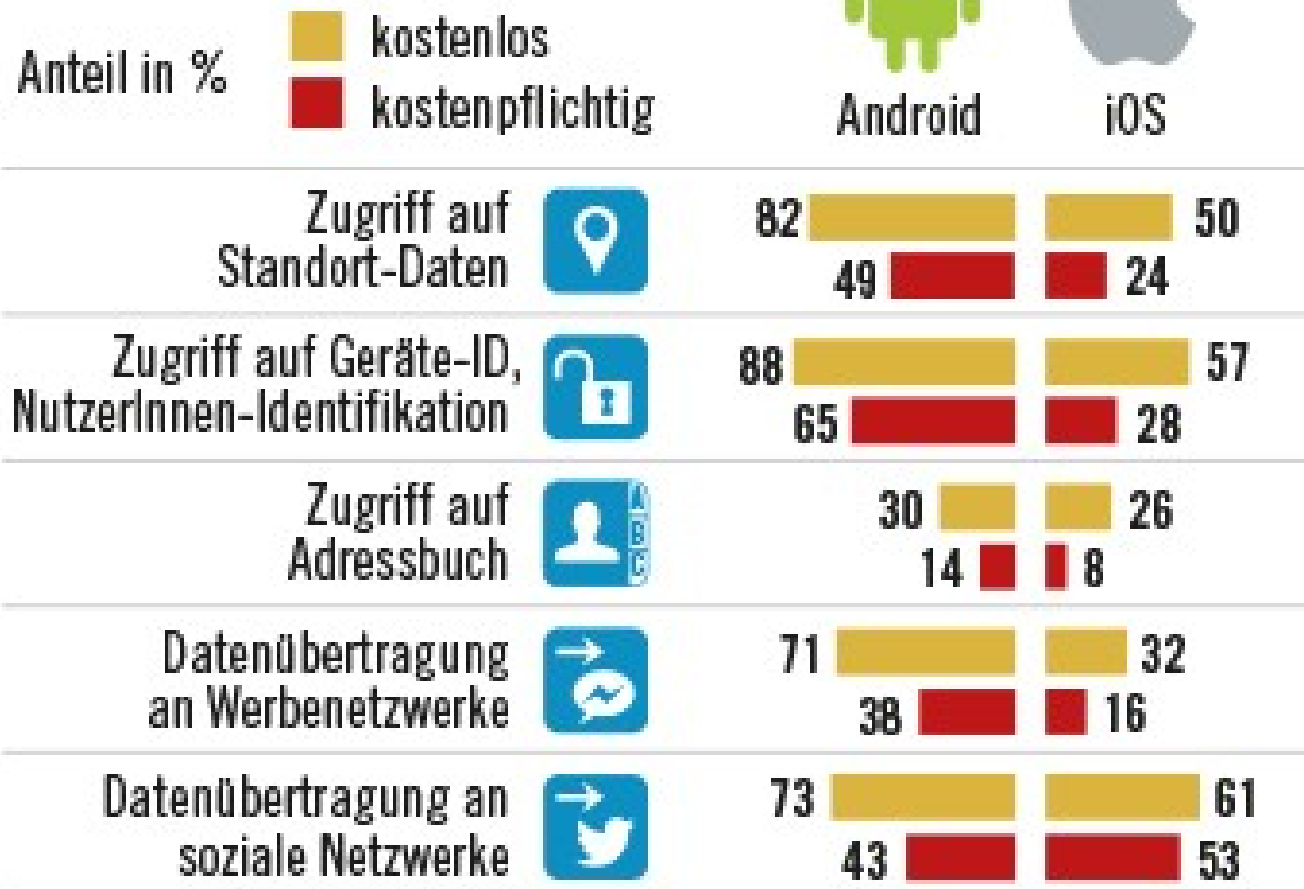
```

Location:



Apps: Spione in der Hosentasche

Top-100-Apps



Untersuchung deutscher Nachrichtenseiten 2014

Die Welt

59

Anzahl der Drittfirmen
auf der Webseite

Bild

44

Spiegel

33

Süddeutsche

47

Zeit online

37

FAZ

55

Tagesspiegel

37

Quelle: Newsreadus.okfn.de



Wer überwacht uns - Kriminelle

Kriminelle, die an unsere **Kennwörter und Bank-Konten** heranwollen („Passwort-Phishing“)

Oder:

Festplatte wird durch Schadprogramm verschlüsselt
(„**Verschlüsselungs-Trojaner**“)

das Entschlüsselungs-Kennwort muß bezahlt werden



Was passiert mit den Daten ?

(Predictive Analytics)



Was passiert mit den Daten ?

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, Banken, Internet-Werbefirmen ...)



Was kann man aus den Daten lesen ?



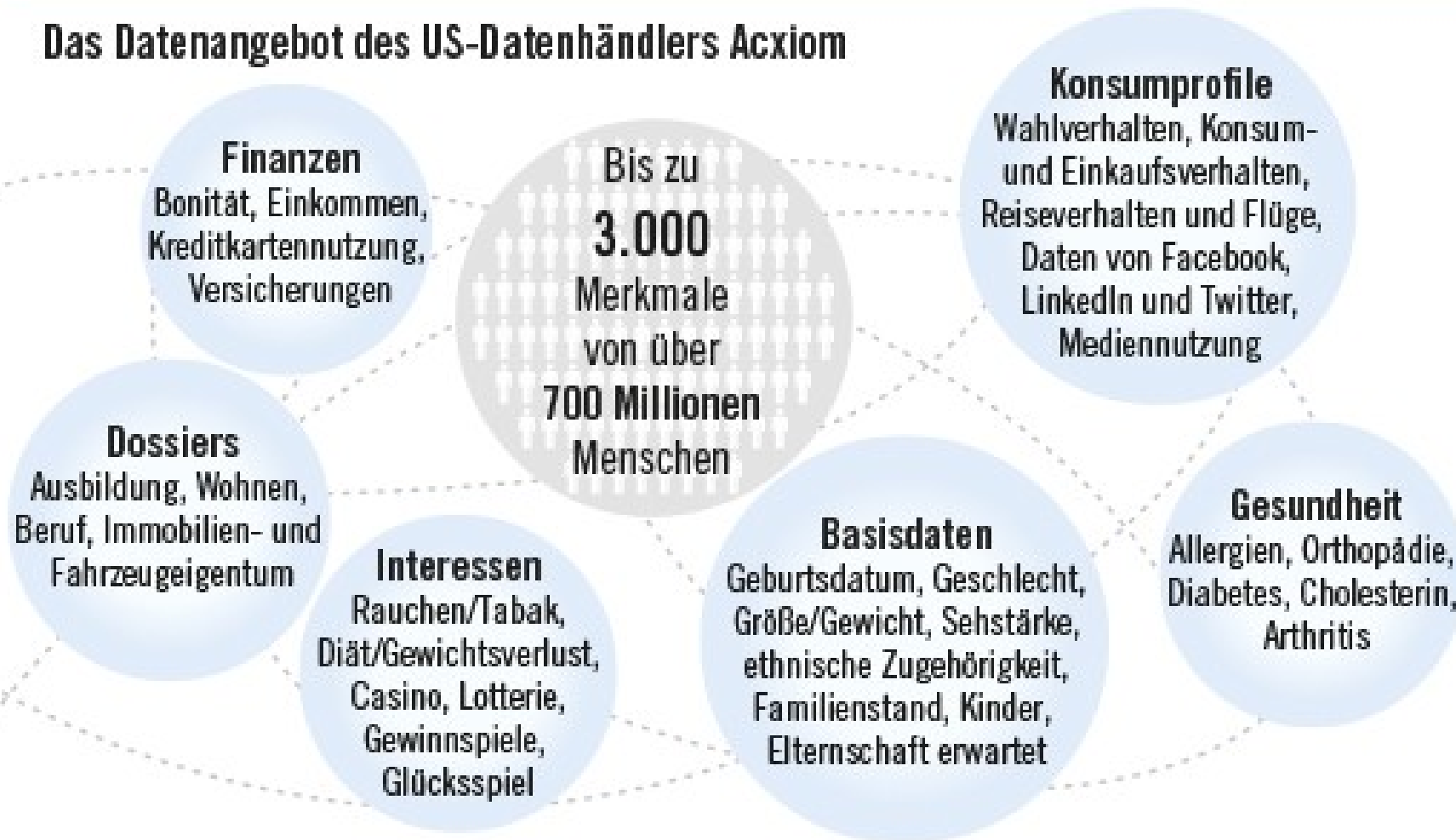
Quelle: www.crackedlabs.org; AK/ÖGB-Darstellung.

ArbeitsWirtschaft 7/2015

ÖGB-VERLAG/ADA-BILDETRACSGRAFIK

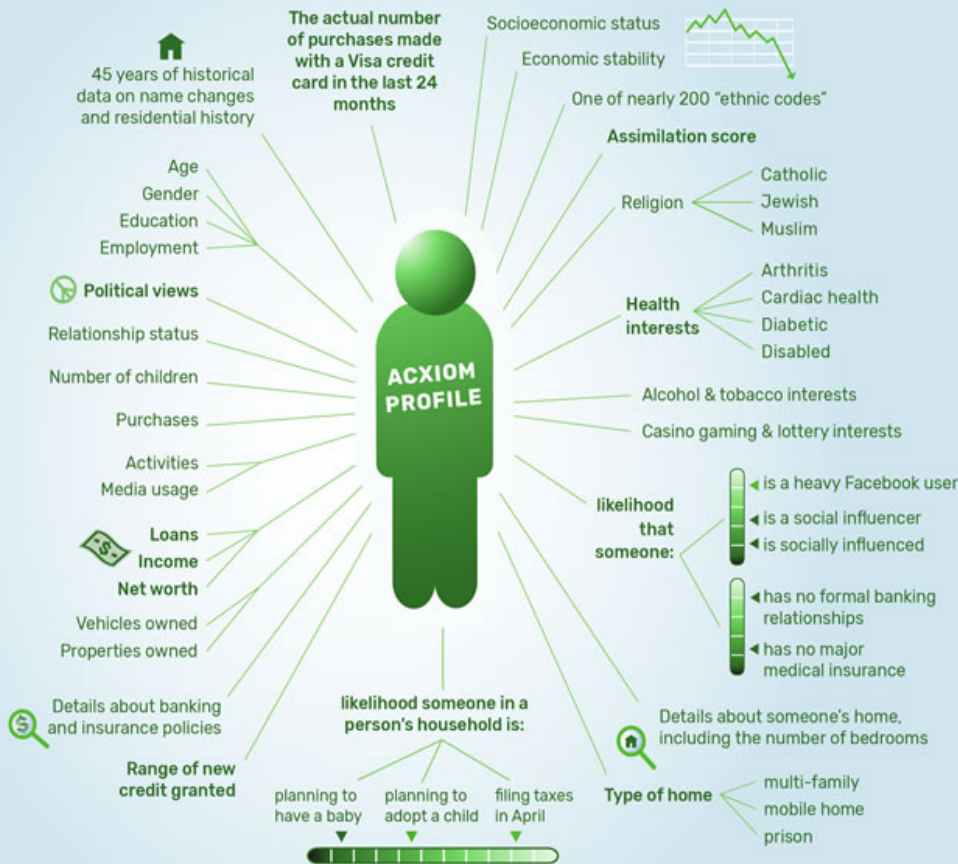
Big Data: Wie wir auf Schritt und Tritt zu kommerziellen Zwecken ausspioniert werden

Das Datenangebot des US-Datenhändlers Acxiom

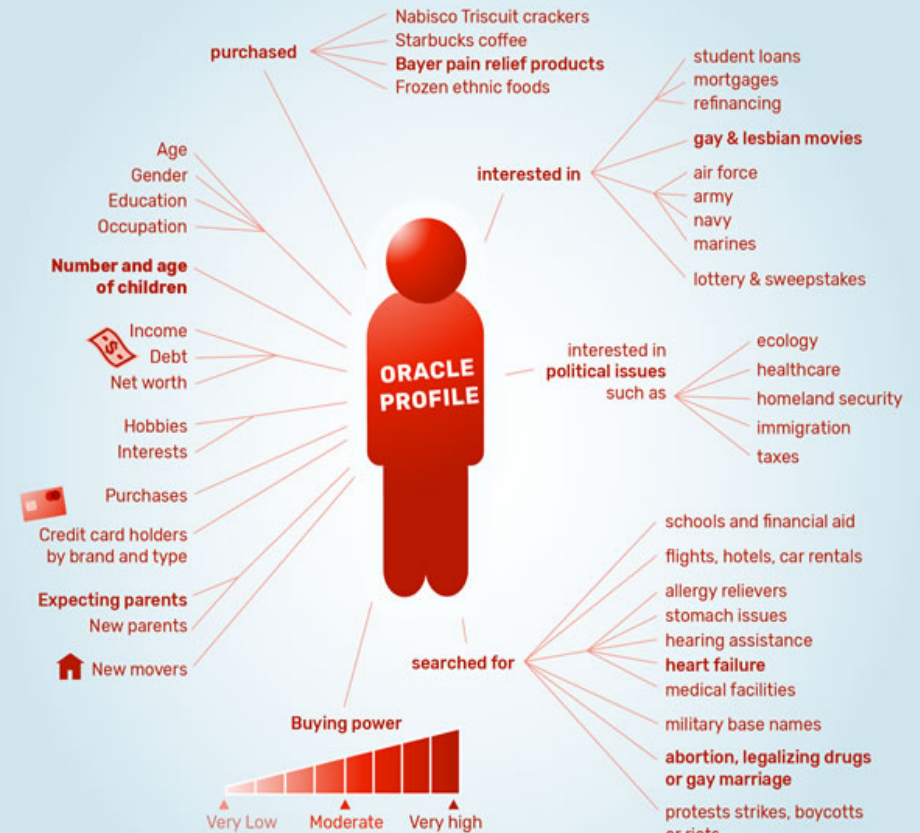


DATA BROKERS HAVE EXTENSIVE PROFILE INFORMATION ON ENTIRE POPULATIONS

Examples of data on consumers provided by Acxiom and Oracle



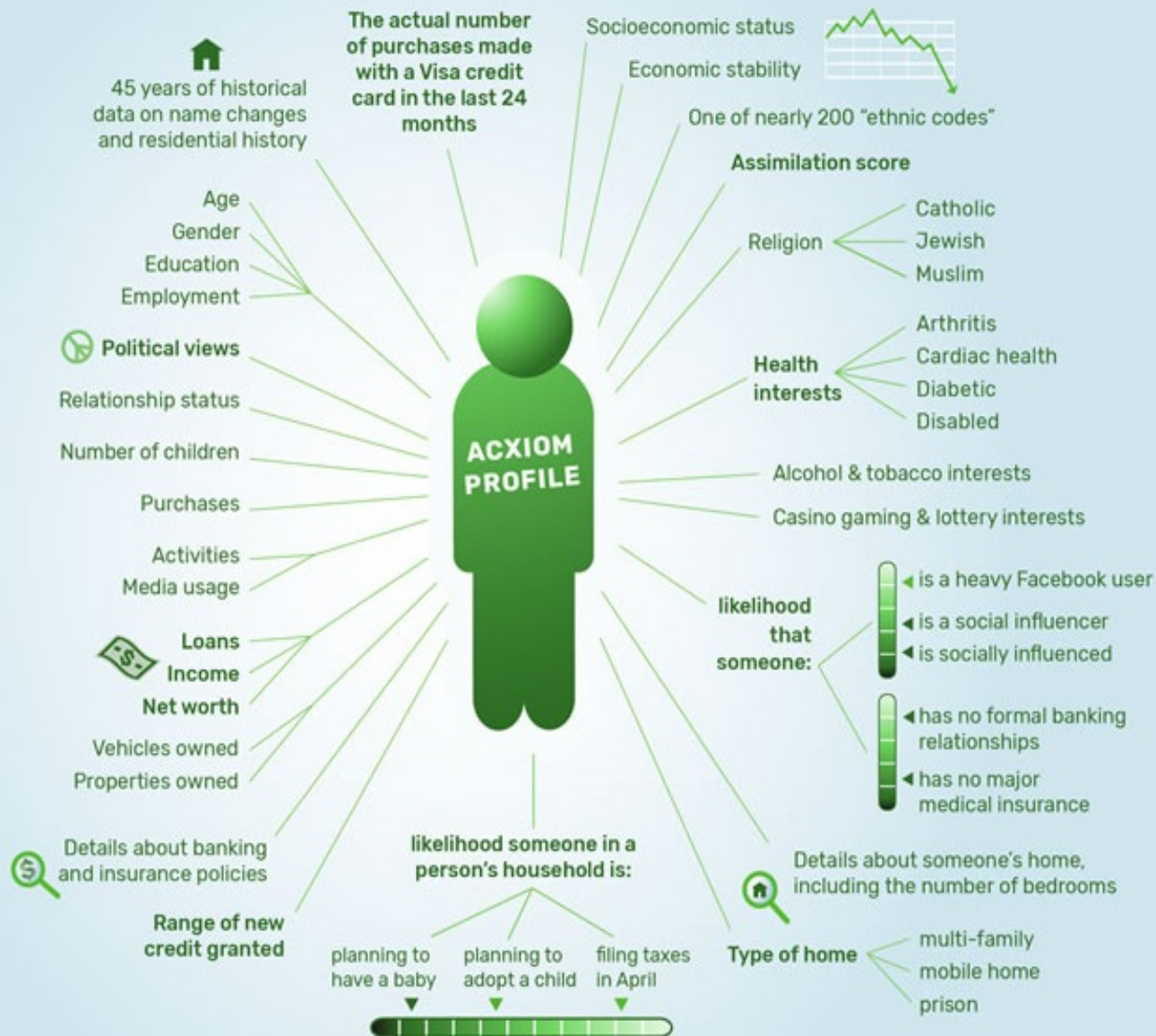
Acxiom provides of up 3,000 attributes and scores on 700 million people in the US, Europe, and other regions.



Oracle sorts people into thousands of categories and provides > 30,000 attributes on 2 billion consumer profiles

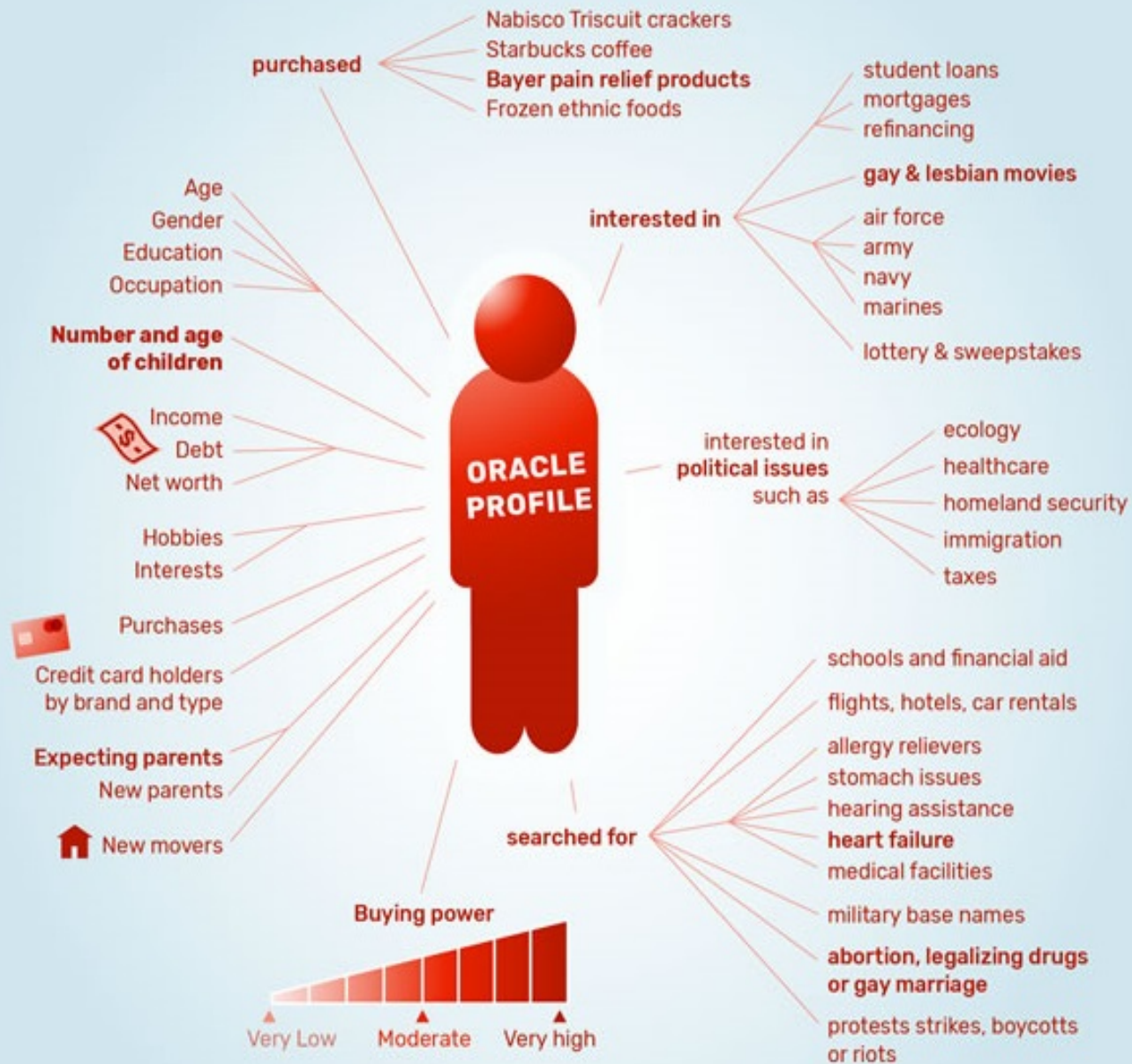
© Cracked Labs CC BY-SA 4.0, April/May 2017. Disclaimer: the mentioned companies typically keep information about their activities secret. This illustration is based on publicly available information by Acxiom and Oracle. Every effort has been made to accurately interpret and represent the companies' activities, but we cannot accept any liability in the case of eventual errors. Sources: Acxiom annual reports, developer website (API docs), Oracle press release, help center website, audience playbook, taxonomy updates for January, 2017 (Excel document). For details about the sources see the report "Corporate Surveillance in Everyday Life".



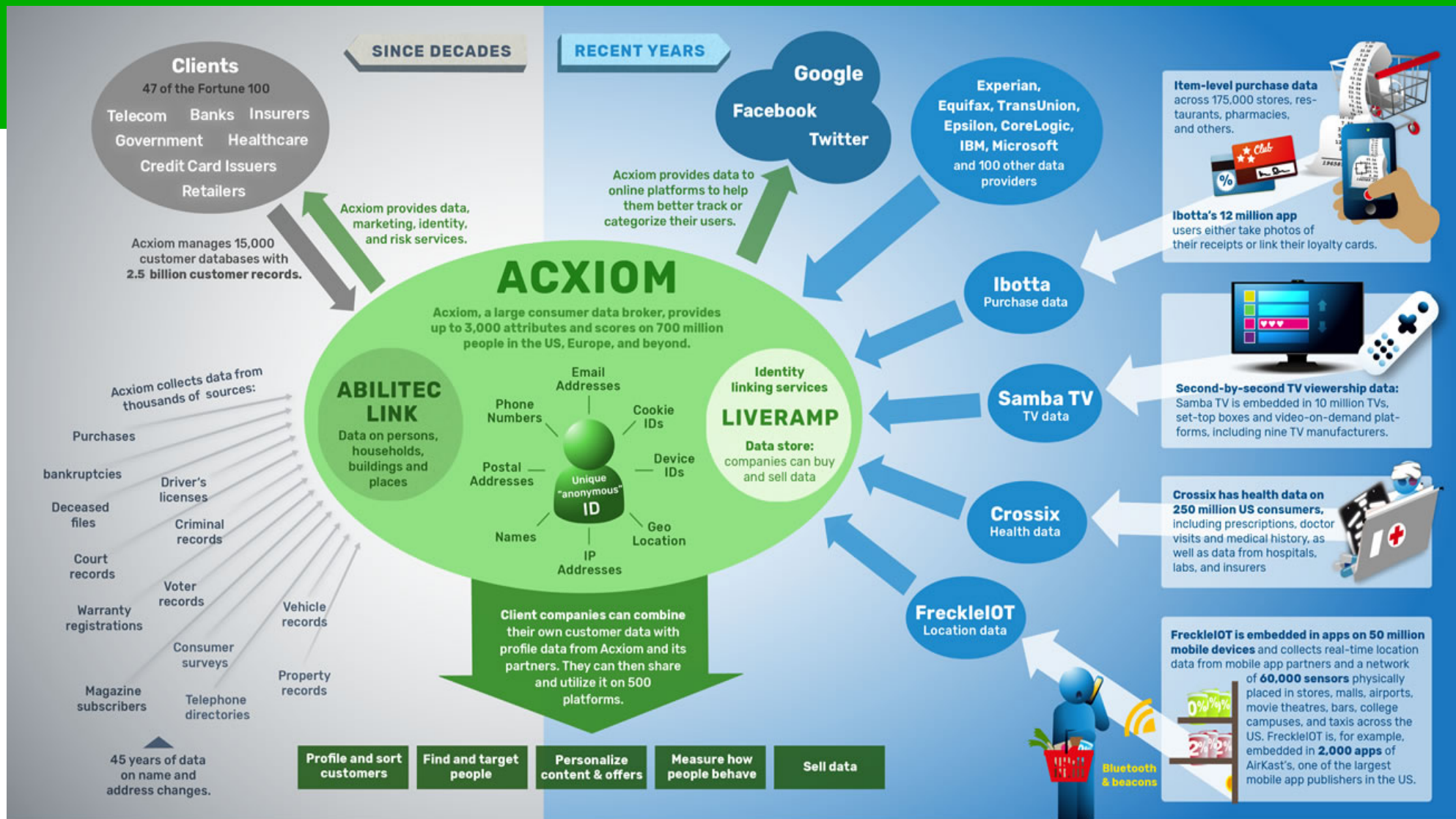


Acxiom provides of up 3,000 attributes and scores on 700 million people in the US, Europe, and other regions.



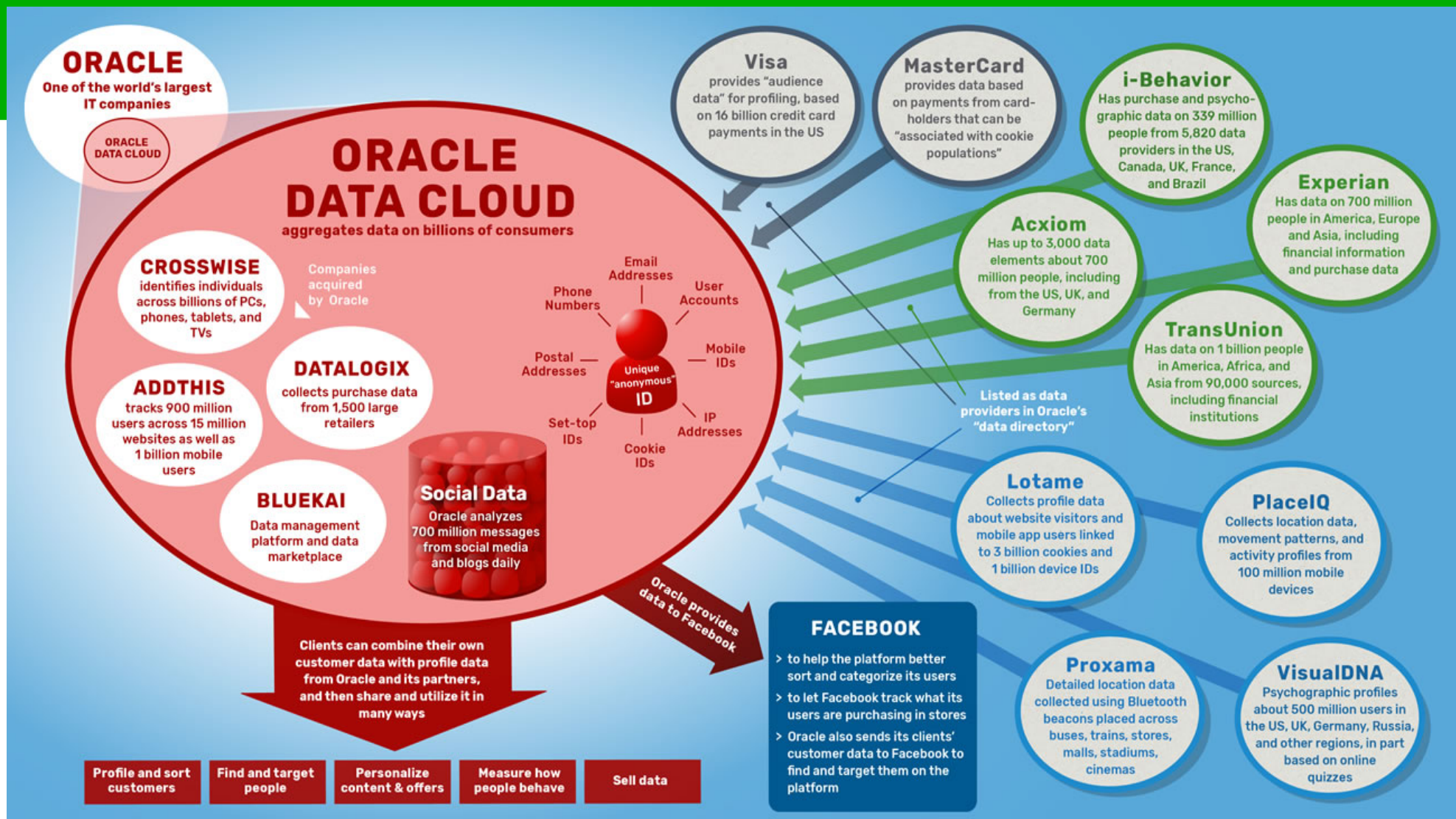


**Oracle sorts people into thousands of categories
and provides > 30,000 attributes on 2 billion consumer profiles**



© Cracked Labs CC BY-SA 4.0, April/May 2017. Disclaimer: the mentioned companies typically keep information about their activities secret. This illustration is based on publicly available information, mainly the companies' own statements. Every effort has been made to accurately interpret and represent the companies' activities, but we cannot accept any liability in the case of eventual errors. Sources: Acxiom website, press releases, brochures, annual reports, and response to US congress inquiry. LiveRamp website, brochures, press releases, presentations. Ibotta website. Crossix website, press releases. FreckleIoT press releases. For details about the sources see the report "Corporate Surveillance in Everyday Life".





© Cracked Labs CC BY-SA 4.0, April/May 2017. Disclaimer: the mentioned companies typically keep information about their activities secret. This illustration is based on publicly available information, mainly the companies' own statements. Every effort has been made to accurately interpret and represent the companies' activities, but we cannot accept any liability in the case of eventual errors. Sources: Oracle website, press releases, data directory, brochures, presentations, MasterCard website, Acxiom annual report, TransUnion annual report, Lotame website, VisualDNA brochure, Facebook website, ProPublica article. For details about the sources see the report "Corporate Surveillance in Everyday Life".



HOW COMPANIES IDENTIFY PEOPLE

to link profile information from various sources and monitor individuals throughout the day

Email addresses and phone numbers are among the most important identifiers used to recognize people.

They are often converted into pseudonyms such as "e907c95ef289bxw2345", which can still serve as personal ID numbers.

Postal addresses have long been used as key nodes for linking consumer data.

Companies often promise to remove names from the collected data. However, names are bad identifiers anyway, at least without further info.

Corporate consumer identifiers, globally unique and ideal for linking all kinds of profile data.

Identifiers related to user accounts on the large platforms play an essential role. Many other user IDs and customer numbers are also relevant.

Many other kinds of temporary identifiers are used to track people across websites, platforms and devices:



People can also be (re)identified through calculating digital fingerprints from behavioral data:



DATA COLLECTION ON CONSUMERS

SINCE DECADES

RECENT YEARS



Name
Birthdate
Postal Address
Phone ZIP

LINKING

CENSUS DATA, MARKET RESEARCH

DATA ABOUT NEIGHBORHOODS & BUILDINGS

HOUSEHOLD-LEVEL DATA

INDIVIDUAL-LEVEL DATA

UNIQUE IDENTIFIERS

YOUR PROFILE

Family Interests
Attitudes Lifestyle
Financial Health
Behaviors Personality
Risk Factors
Weaknesses
Movements



Profile data is stored by many companies from retailers to data brokers to online platforms.

AGGREGATED, ANONYMIZED "BIG DATA"

METADATA ABOUT WEBSITES, APPS, CONTENT, PLACES

BROWSER OR DEVICE SPECIFIC DATA

INDIVIDUAL-LEVEL DATA

UNIQUE IDENTIFIERS

Location
Device IDs
Accounts Email
Cookie IDs

LINKING

Publicly available data on the web

Website visits, searches and other behaviors

Social media, platforms and user accounts

Smartphone and app usage

Online Purchases

Smart TVs, activity trackers, game consoles, e-readers, cars and other devices

© Cracked Labs CC BY-SA 4.0

Der Datenhändler Acxiom

„Acxiom erhebt personenbezogene Daten wie Name, Post- und E-Mail-Adresse, Telefonnummer, Reaktionsdaten, Lifestyle- und demographische Daten sowohl online als auch offline über Fragebögen und Werbezusendungen direkt beim Betroffenen, über unsere Partnerunternehmen, aus öffentlich zugänglichen Quellen, aus kommerziellen Datenbanken und über unsere Webseite.

Personenbezogene Daten können in identifizierter Form oder als aggregierte Daten (damit Einzelpersonen nicht erkannt werden können) gehalten und für die nachfolgend aufgeführten Zwecke verwendet werden.“

<http://d1fe5u1jnbojul.cloudfront.net/wp-content/uploads/2015/11/Acxiom-Datenschutzrichtlinie.pdf>

Acxiom ist ein privates Unternehmen, das allerdings der US-Regierung nach 9/11 beim Aufbau von Systemen half.

http://www.zero-das-buch.de/big_brother.php



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

Konsequenzen ?



Konsequenzen - konkret

- Werbung
- Preisanpassung (Urlaubsbuchung, Supermarkt)
- Empfohlene Inhalte
- Versicherungstarife
- ...



Konsequenzen - allgemein

- Kontrollverlust
- Mangel an Transparenz
- Machtungleichheit
- Fehlerhafte Daten, fehlerhafte Prognosen
- Datenmissbrauch
- Identitätsdiebstahl
- Bedrohung von
 - Freiheit
 - Demokratie
 - Autonomie des Einzelnen



COMMERCIAL DIGITAL TRACKING AND PROFILING LANDSCAPE

In recent years,
most industries
have joined today's
pervasive personal
data ecosystems

TELCO/MEDIA
Verizon
AOL, Yahoo
Comcast
NBC Universal
AT&T
TimeWarner

**MEDIA AND
PUBLISHING**
Online Publishers
Video
Games
Websites
Music
Apps
Walt Disney
Grupo Globo
CBS
Bertelsmann
News Corp
Viacom
Asahi Shimbun

Companies in many sectors
seamlessly gather, analyze,
share, trade, and utilize
data on billions

**RETAIL, CONSUMER
GOODS AND SERVICES**
Online Shops
Retail
Grocery
Pharmacies
Brands
Automotive
Travel & Hospitality
Mail Order

**TELECOM, DEVICE, AND
SERVICE PROVIDERS**
Airtel
Mobile Carriers
ISPs
Telenor
Telefónica
China Mobile
Samsung
Wearables
Smart Home
IoT
Connected Car

**LARGE
PLATFORMS**
Google
Facebook
Alibaba
Amazon
Baidu
Apple
eBay
Microsoft
Tencent
Naspers
Softbank

Large-scale collection
and use of data on
people, often without
their knowledge

CONSUMER DATA AND ANALYTICS INDUSTRY

ADVERTISING TECHNOLOGY
SSPs
Ad Networks
Turn
Nielsen
Neustar
Rocket Fuel
DSPs
DMPs
Personalization
MailChimp
Predictive Marketing
Cross-device tracking
CRM
Salesforce
Epsilon
Merkle
Acxiom
Database Services
Segmentation
Agencies
WPP
List Rental
Lead Generation
Marketing Data
Direct Marketing
Experian
TransUnion
Equifax
ID Analytics
Telematics Data
Cyber Security
Credit Scoring
LexisNexis
Background Checks
Risk Data
Fraud Detection
Palantir
FICO
SAS
Health & Insurance Analytics
Auth
IBM
Oracle
McKinsey
Accenture
Deloitte
Managed Services
Microsoft

CUSTOMER MANAGEMENT
Loyalty Programs
Call Center
Personalization
MailChimp
Predictive Marketing
Cross-device tracking
CRM
Salesforce
Epsilon
Merkle
Acxiom
Database Services
Segmentation
Agencies
WPP
List Rental
Lead Generation
Marketing Data
Direct Marketing
Experian
TransUnion
Equifax
ID Analytics
Telematics Data
Cyber Security
Credit Scoring
LexisNexis
Background Checks
Risk Data
Fraud Detection
Palantir
FICO
SAS
Health & Insurance Analytics
Auth
IBM
Oracle
McKinsey
Accenture
Deloitte
Managed Services
Microsoft

DATA INTEGRATION AND IDENTITY MATCHING

FINANCIAL SERVICES
Payment Services
Credit Card Companies
Services Brokers
Fintech
Collection Agencies
Lenders
Banks & Insurers
Leasing
Investigations

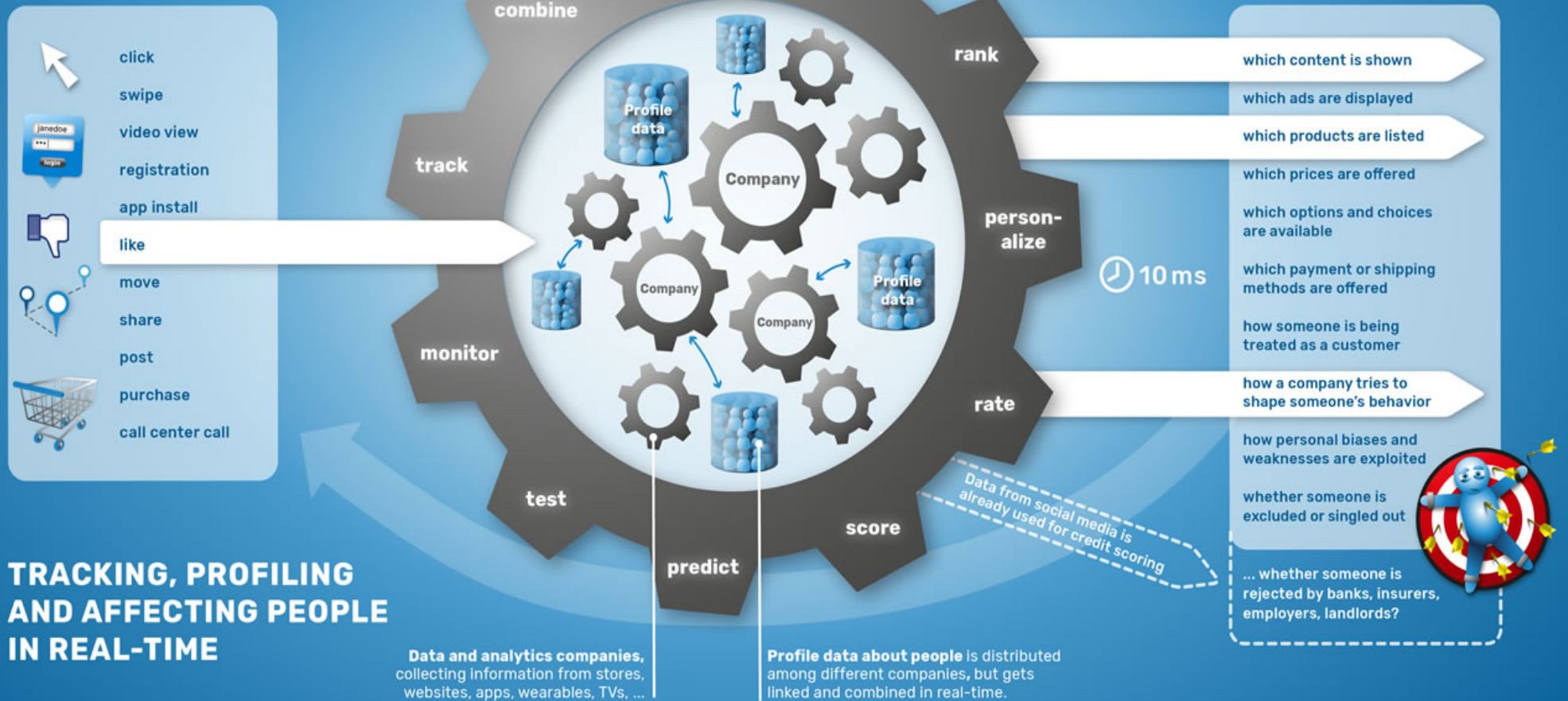
**PUBLIC SECTOR AND
KEY SOCIETAL DOMAINS**
Politics
Science
Utilities & Energy
Advocacy
Education
Law
Welfare
Housing
Enforcement
Employment
Healthcare

**GOVERNMENT
SURVEILLANCE**

EVERY INTERACTION...

...TRIGGERS A WIDE RANGE OF DATA FLOWS BETWEEN MULTIPLE COMPANIES

...AND CAN AFFECT:



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

Gesamt-Score

40 % Fahrweise

Berechnungsregeln

- 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 $0,235 \text{ g} = 2,3 \text{ m/s}^2$ ** mehr als $0,286 \text{ g} = 2,8 \text{ m/s}^2$

Studie: Kommerzielle digitale Überwachung im Alltag (2014)

Erfassung, Verknüpfung und Verwertung persönlicher Daten im Zeitalter von Big Data: Internationale Trends, Risiken und Herausforderungen anhand ausgewählter Problemfelder und Beispiele.

Wien, November 2014. Projektleitung und Autor: Wolfie Christl. Eine Studie von Cracked Labs im Auftrag der österreichischen Bundesarbeitskammer.

Download der Studie:

- Vollständige Version: http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf
- Kurzfassung: http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung_Kurzfassung.pdf

» Online-Version : <http://crackedlabs.org/studie-kommerzielle-ueberwachung>



Buch: Networks of Control (2015)

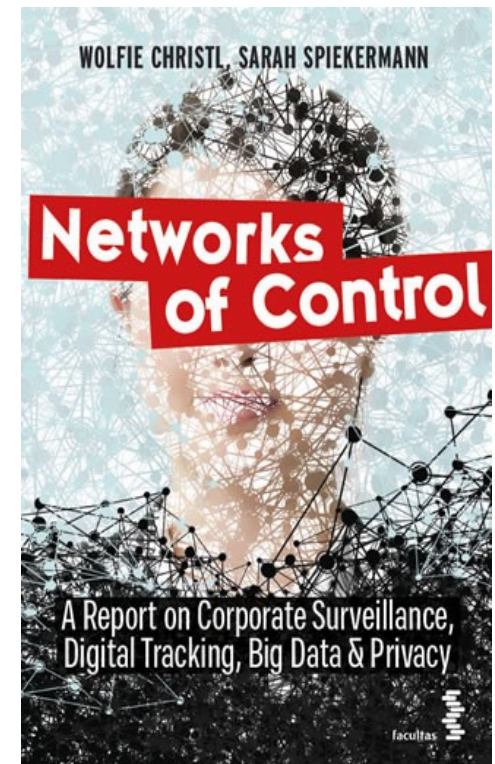
A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy

by Wolfie Christl and Sarah Spiekermann

Download :

- http://crackedlabs.org/dl/Christl_Spiekermann_Networks_Of_Control.pdf

<http://crackedlabs.org/en/networksofcontrol>



Studie: Corporate Surveillance in Everyday Life (2017)

Report and web publication on how companies collect, analyze, and use personal data.

June 2017



Download der Studie:

- http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

<http://crackedlabs.org/en/corporate-surveillance>



Studie: How Companies Use Personal Data Against People (2017)

Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information.

Working paper by Cracked Labs, October 2017.

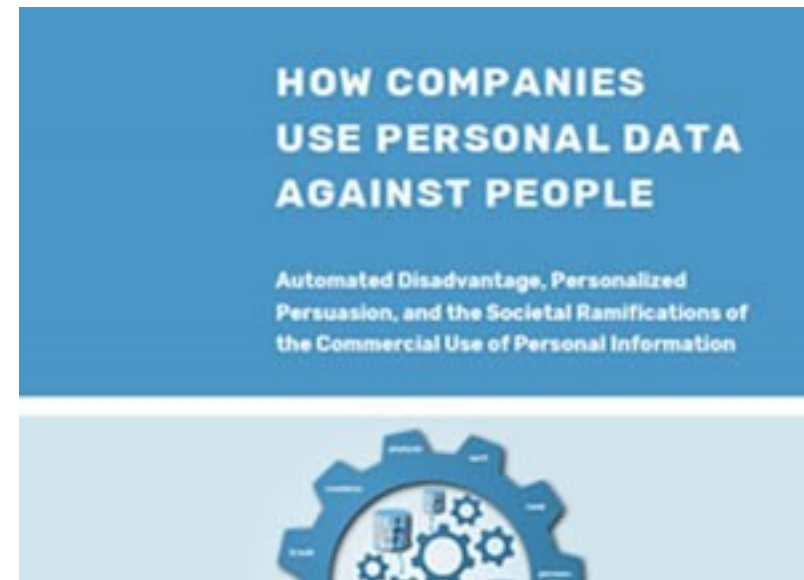
Author: Wolfie Christl.

Contributors: Katharina Kopp, Patrick Urs Riechert.

Download der Studie:

• http://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf

<http://crackedlabs.org/en/data-against-people>



Was kann man als Gegenmassnahmen tun ?



Was tun – auf einer Folie

- **Andere Suchmaschinen nutzen**, die keine persönlichen Daten speichern
- **Web-Browser-Plugins** gegen Web-Tracking installieren
- **Updates installieren**

152 Tipps von Experten

Reeder / Iulia Ion / Consolvo 2017

50 Tipps (5 Verteidigungsstufen)

Heuer / Tranberg 2015



Datenschutzfreundliche Suchmaschinen

Startpage Privates, aufzeichnungsfreies Websuchen. https://startpage.com		DuckDuckGo Privates, aufzeichnungsfreies Websuchen https://duckduckgo.com	
MetaGer Meta-Suchmaschine, die Suchanfragen an verschiedene Suchanbieter weiterleitet. https://metager.de		Ixquick Ixquick ist eine Metasuchmaschine. https://ixquick.eu	



SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES

VS

SECURITY EXPERTS' TOP ONLINE SAFETY PRACTICES

1. USE ANTIVIRUS
SOFTWARE



2. USE STRONG
PASSWORDS



3. CHANGE PASSWORDS
FREQUENTLY



4. ONLY VISIT WEBSITES
THEY KNOW



5. DON'T SHARE
PERSONAL INFORMATION



1. INSTALL SOFTWARE
UPDATES



2. USE UNIQUE
PASSWORDS

2

3. USE TWO-FACTOR
AUTHENTICATION



4. USE STRONG
PASSWORDS



5. USE A PASSWORD
MANAGER

152 Simple Steps to Stay Safe Online

Security Advice for Non-Tech-Savvy Users

Robert W. Reeder, Iulia Ion, Sunny Consolvo

Google

IEEE Security & Privacy, vol. 15, no. , pp. 55-64

September/October 2017

<https://research.google.com/pubs/archive/46306.pdf>

<https://www.computer.org/csdl/mags/sp/2017/05/msp2017050055-abs.html>



230 Sicherheitsexperten befragt;
sie mussten ihre 3 wichtigsten Tipps für Computer-
Sicherheit nennen, die sie Nicht-Experten geben
würden

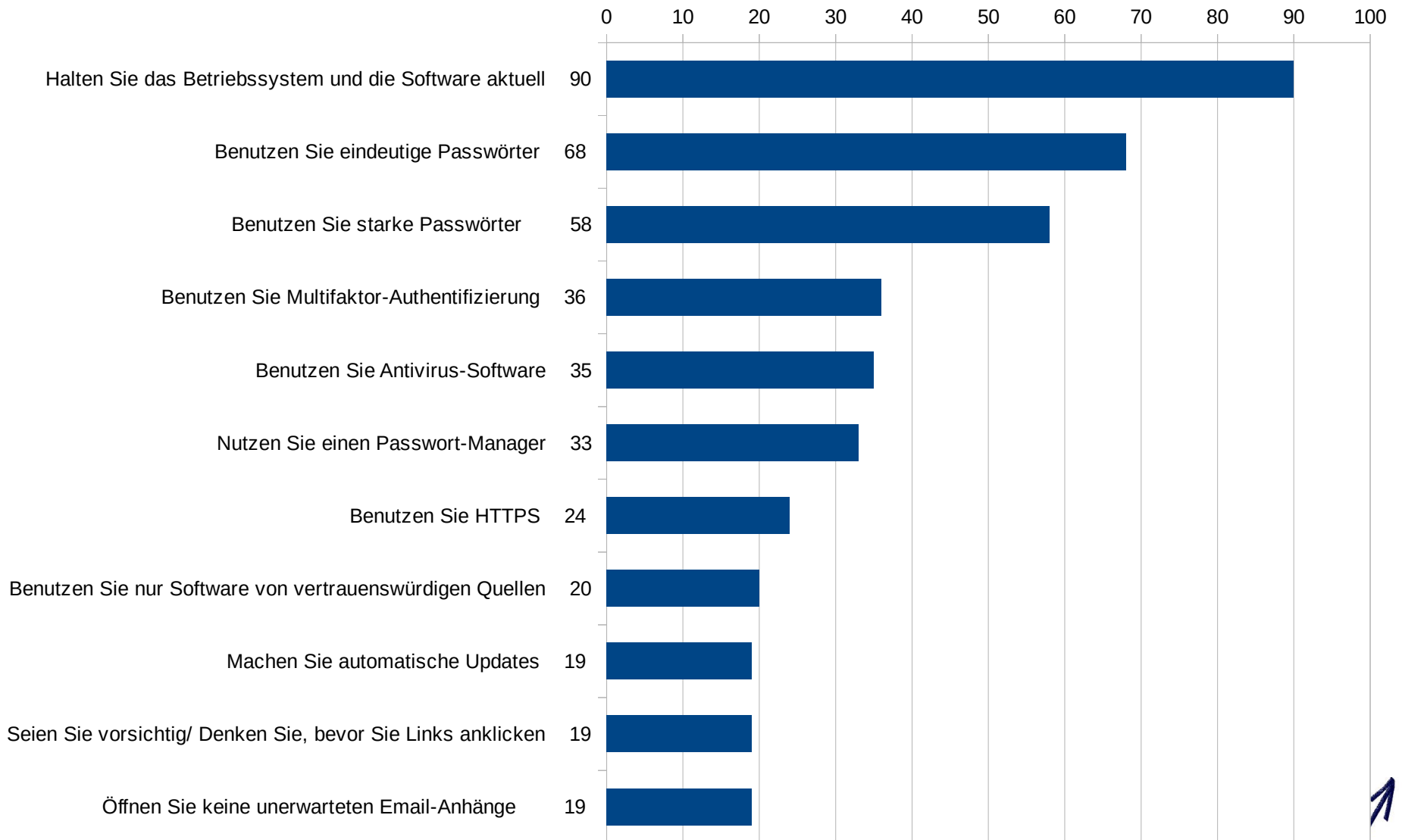
<https://security.googleblog.com/2015/07/new-research-comparing-how-security.html>



Die 10 meistgenannten Hinweise

Halten Sie das Betriebssystem und die Software aktuell	90
Benutzen Sie eindeutige Passwörter	68
Benutzen Sie starke Passwörter	58
Benutzen Sie Multifaktor-Authentifizierung	36
Benutzen Sie Antivirus-Software	35
Nutzen Sie einen Passwort-Manager	33
Benutzen Sie HTTPS	24
Benutzen Sie nur Software von vertrauenswürdigen Quellen	20
Machen Sie automatische Updates	19
Seien Sie vorsichtig / Denken Sie, bevor Sie Links anklicken	19
Öffnen Sie keine unerwarteten Email-Anhänge	19





Die 45 am häufigsten genannten Tipps

Account Sicherheit	128
Updates	97
Verhalten beim Web-Browsen	76
Verhalten bei Email	59
Achtsamkeit	42
Antivirus	41
Privacy	30
Browser Software	29
Geräte Sicherheit	24
Software Sicherheit	22
Netzwerk Sicherheit	15
Backups / Datensicherungen	10
Ausbildung / Erziehung	11
Betriebssysteme	99



Account Sicherheit

- Benutze eindeutige Passwörter, für jeden Account ein anderes
- Benutze starke Passwörter
- Benutze Multifaktor Authentifizierung
- Benutze einen Passwort-Manager
- Benutze eine Pass-Phrase
- Schreibe dir deine Passwörter auf
- andere Sicherheitsmassnahmen ...



Updates

- Halte dein System und die Software aktuell
- Mache automatische Updates
- Anderes ...



Surf-Verhalten

- Verwende HTTPS
- Sei vorsichtig / denke, bevor du auf einen Link klickst
- Überprüfe, ob die URL zur richtigen Seite führt
- Überprüfe den Link, bevor du darauf klickst
- Private Informationen nur über HTTPS angeben
- Überprüfe das Schloss-Icon
- Passe bei Sicherheitswarnungen auf
- Schaue, ob es HTTPS in der URL gibt
- Besuche nur Webseiten mit Reputation
- Anderes ...



Email-Verhalten

- Öffne keine unerwarteten Anhänge
- Klicke überhaupt nie auf Links in Emails
- Klicke nicht auf Links in Emails von unbekannten Absendern
- Sei bei Emails generell vorsichtig
- Hüte dich vor Phishing-Mails
- Seie skeptisch bei Emails, die persönliche Daten verlangen
- Sei sogar bei Emails von bekannten Absendern vorsichtig
- Anderes Email-Verhalten



Achtsamkeit

- Sei generell skeptisch
- Sei bei "zu gut um wahr zu sein"-Angeboten skeptisch
- Verwende den gesunden Hausverstand
- Anderes ...



Antivirus

- Benutze Antivirus-Software
- Halte Antivirus-Software aktuell
- Anderes ...



Privatheit

- Schränke das Teilen von persönlichen Informationen ein
- Sei vorsichtig, was du teilst
- Anderes ...



Browser-Software

- Benutze Chrome
- Benutze einen Werbe-Blocker
- Benutze kein Java
- Anderes ...



Geräte-Sicherheit

- Arbeite nicht als Administrator
- Mache sensitive Arbeiten nur auf speziellen Geräten
- Mache sensitive Arbeiten nur auf vertrauenswürdigen Geräten
- Sperre Geräte ab
- Anderes ...



Netzwerk-Sicherheit

- Traue offenen Netzwerken nicht
- Anderes ...



Backups

- Mache von deinen Daten regelmäßige Backups
- Anderes ...



Ausbildung / Erziehung

- Lerne über Sicherheits-Themen
- Kontaktiere Experten, wenn Hilfe nötig ist
- Anderes ...



Betriebssystem

- Benutze ein wenig verbreitetes Betriebssystem
- Anderes ...



50 Tipps in 5 Stufen



Steffan Heuer
Pernille Tranberg

Mich kriegt ihr nicht !

Murmann Verlag 2015

<http://www.murmann-verlag.de/mich-kriegt-ihr-nicht-31242.html>

<http://www.digital-selfdefense.com/>



Verteidigungsstufe I :

Die 10 grundlegenden Dinge, die Sie tun sollten

- 1) Löschen Sie Cookies und das Webprotokoll**
- 2) Verwenden Sie Google-Datenschutz-Werkzeuge,
aber vermeiden Sie es zu häufig Google zu benutzen**
- 3) Diese Informationen gehören nicht in Soziale Netze**
- 4) Verwenden Sie mehrere Web-Browser**
- 5) Verwenden Sie Pseudonyme für Ihr privates Ich**
- 6) Grundlegende Sicherheit bei facebook**
- 7) Grundlegende mobile Sicherheit**
- 8) Schützen Sie Ihre Emails**
- 9) Verwenden und merken Sie sich sichere Passwörter**
- 10) Kaufen Sie sicher mit Ihrer Kreditkarte ein**



Verteidigungsstufe II :

Die nächsten 10 Dinge, die Sie tun sollten

- 11) Verwenden Sie Blocking-Werkzeuge in Ihrem Web-Browser**
- 12) Verwenden Sie privates Surfen**
- 13) Verwenden Sie Firefox zum Porno-Surfen**
- 14) Sperren Sie Social Widgets**
- 15) Fortgeschrittene Sicherheit bei facebook**
- 16) Sicherheit bei mobilen Apps**
- 17) Verbergen Sie Ihre IP-Adresse mit einem VPN**
- 18) Säubern Sie Ihre Online-Reputation**
- 19) Beugen Sie Identitätsdiebstahl vor**
- 20) Säubern Sie Ihren Rechner**



Verteidigungsstufe III :

Die nächsten 10 Dinge, die Sie tun sollten

- 21) Sichern Sie Ihre Fotos**
- 22) Verschlüsseln Sie Ihre Korrespondenz - die Grundlagen**
- 23) Surfen Sie mit Verschlüsselung**
- 24) Verschlüsseln Sie Ihre Chats**
- 25) Verschlüsseln Sie Ihre Beiträge auf Sozialen Netzwerken**
- 26) Mobile Sicherheit für Fortgeschrittene**
- 27) Verschlüsseln Sie Ihre Festplatten**
- 28) Entfernen Sie Ihren digitalen Spuren**
- 29) Manchmal hilft nur der Hammer**
- 30) Löschen Sie Ihr facebook-Profil**



Verteidigungsstufe IV :

Zehn Dinge, um Spionen das Leben schwer zu machen

- 31) Meiden Sie US-Dienstleister und US-Software**
- 32) Verschlüsseln Sie Ihre Daten im Ruhezustand**
- 33) Verschlüsseln Sie Ihre Kommunikation von A bis Z**
- 34) Nichtamerikanische Email-Dienste**
- 35) Nichtamerikanische Suchmaschinen**
- 36) Nichtamerikanische Hosting-Anbieter und Cloud-Dienste**
- 37) Das Trio: Verwenden Sie VPNs und Anonymisierung plus Verschlüsselung**
- 38) Vergängliche Alternativen zu E-Mail**
- 39) Verzichten Sie auf Ihr Smartphone**
- 40) Verzichten Sie auf Kreditkarten**



Verteidigungsstufe V :

Der Rest

- 41) Entfernen Sie die Kennung Ihres Handys
- 42) Verwenden Sie Einwegtelefonnummern
- 43) Verwenden Sie Fingerabdruck-Authentifizierung und Passwörter vom USB-Stick
- 44) Überprüfen Sie Ihren Browser-Fingerabdruck
- 45) So begehen Sie Selbstmord auf Twitter
- 46) Säubern Sie Ihr YouTube-Konto
- 47) Das ist nicht cool - Medienkompetenz für Kinder
- 48) Sollte man Passwörter wiederverwenden?
- 49) Gönnen Sie sich eine Pause von der digitalen Welt
- 50) Bereiten Sie Ihr digitales Erbe vor



Literatur

- Wolfie Christl 2014, 2015, 2017
- Mich kriegt ihr nicht
- Privacy-Handbuch
- ISPA-Broschüren
- Selbstdatenschutz - BLM
- Clemens Kommerell
- Tobias Schrödel



Literatur



Steffan Heuer
Pernille Tranberg

Mich kriegt ihr nicht !

Murmann Verlag 2015

<http://www.murmann-verlag.de/mich-kriegt-ihr-nicht-31242.html>

<http://www.digital-selfdefense.com/>



Literatur

Privacy-Handbuch

- Eher schon für technisch Versierte
- <https://privacy-handbuch.de/download/privacy-handbuch.pdf>
- https://privacy-handbuch.de/download/privacy-handbuch_win.pdf

ISPA-Broschüren

- <https://www.ispa.at/wissenspool/broschueren.html>
- z.B.:
 - Internet sicher nutzen,
 - Sicherheitseinstellungen für mobile Endgeräte



Selbstdatenschutz !

Broschüre des BLM (Bayrische Landeszentrale für Neue Medien) 2016

<https://www.blm.de/files/pdf1/blm-selbstschutz.pdf>

Und auch die Webseite

www.selbstdatenschutz.info



Literatur

Clemens Kommerell: Du hast nichts zu verbergen?

- Erste Schritte zur Digitalen Selbstverteidigung, Zürich 2016
- https://cdn.netzpolitik.org/wp-upload/2016/12/Kommerell_Du-hast-nichts-zu-verbergen.pdf



Tobias Schrödel: Ich glaube, es hackt!

Springer 2016

- Sehr unterhaltsam und gut verständlich
- <http://sichere.it/de/index.php#buch>
- <http://ich-glaube-es-hackt.de/>
-



Bildquellen:

Wolfie Christl, Corporate Surveillance in Everyday Life,
2017

<http://crackedlabs.org/en/corporate-surveillance>

